10/665,484

7

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　９月　５日

出願番号
Application Number: 特願２００３－３１４４６５

[ST. 10/C]: [ＪＰ２００３－３１４４６５]

出願人
Applicant(s): 株式会社リコー

２００３年１０月　７日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０８２７２７

【書類名】　特許願
【整理番号】　0304621
【提出日】　平成15年 9月 5日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　斉藤　敦久
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　金井　洋一
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　谷内田　益義
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-273985
　【出願日】　平成14年 9月19日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-275973
　【出願日】　平成14年 9月20日
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-297888
　【出願日】　平成14年10月10日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、
外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、
上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有することを特徴とする画像形成装置。
【請求項２】
ネットワークを介して通信制御を行う通信手段を有し、
上記ポリシー書き換え手段は、上記通信手段によって受信したセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項１記載の画像形成装置。
【請求項３】
上記ポリシー書き換え手段は、電源投入時に上記通信手段によって、外部から取得したセキュリティポリシーを上記ポリシー保持手段に書き込むことを特徴とする請求項２記載の画像形成装置。
【請求項４】
上記ポリシー保持手段にて保持される上記セキュリティポリシーの書き換えタイミングを上記通信手段に通知するタイマー手段を有し、
上記通信手段は、上記ネットワークを介して、上記セキュリティポリシーを配布するポリシー配布サーバから該セキュリティポリシーを取得することを特徴とする請求項２又は３記載の画像形成装置。
【請求項５】
セキュリティポリシーを記憶した記憶媒体から該セキュリティポリシーを読み出すインターフェース手段を有し、
上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項１記載の画像形成装置。
【請求項６】
ネットワークを介して通信制御を行う通信手段を有し、
上記通信手段は、セキュリティポリシーの選択を示す選択情報を受信すると、上記ポリシー書き換え手段に通知し、
上記ポリシー書き換え手段は、上記選択情報に基づいて、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えることを特徴とする請求項５記載の画像形成装置。
【請求項７】
上記ポリシー保持手段は、複数のセキュリティポリシーを保持し、
上記ポリシー書き換え手段は、上記選択情報に基づいて、上記ポリシー保持手段で保持される上記複数のセキュリティポリシーの１つを施行すべきセキュリティポリシーとして設定することを特徴とする請求項６記載の画像形成装置。
【請求項８】
上記通信手段は、上記ネットワークを介して、Simple Object Access Protocolに従って上記セキュリティポリシーを取得することを特徴とする請求項２又は６記載の画像形成装置。
【請求項９】
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手順と、

外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、
上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータが実行することを特徴とする方法。
【請求項１０】
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手順と、
外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、
上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能なプログラム。
【請求項１１】
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手順と、
外部からのセキュリティポリシーで上記ポリシー保持手順にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手順と、
上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手順とをコンピュータに実行させることを特徴とするプログラムが記憶されたコンピュータ読み取り可能な記憶媒体。
【請求項１２】
ネットワークを介して通信制御を行う通信手段と、
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを管理するポリシー管理手段とを有し、
上記通信手段は、上記ポリシー管理手段によって管理される上記セキュリティポリシーを上記ネットワークを介して接続される装置へ配布することを特徴とするポリシー配布サーバ。
【請求項１３】
上記通信手段は、上記セキュリティポリシーを配布する際に、認証情報を同時に送信することを特徴とする請求項１２記載のポリシー配布サーバ。
【請求項１４】
上記通信手段は、上記ネットワークを介して接続される上記装置から上記ポリシー管理手段によって管理される上記セキュリティポリシーの取得要求と共に、該装置の認証情報とを受信し、該認証情報に基づいた認証結果に従って、該装置へ該セキュリティポリシーを送信することを特徴とするポリシー配布サーバ。
【請求項１５】
記憶媒体へ上記セキュリティポリシーを書き込むインターフェースを有し、
上記ポリシー管理手段は、上記インターフェースによって、上記セキュリティポリシーを上記記憶媒体に書き込むことを特徴とする請求項１２乃至１４のいずれか一項記載のポリシー配布サーバ。
【請求項１６】
ドキュメントに関するドキュメント属性を、該ドキュメント属性に基づいて該ドキュメントに関する取り扱いのルールを提供する外部サーバへ送信することによって、該外部サーバから上記ルールを取得するルール取得手段と、
上記ルール取得手段によって取得された上記ルールに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有することを特徴とする画像形成装置。
【請求項１７】
上記ルール取得手段は、上記外部サーバとの通信をSimple Object Access Protocolに従って制御する通信手段を有することを特徴とする請求項１６記載の画像形成装置。

【請求項１８】
上記ルール取得手段は、
上記外部サーバとの通信を制御する通信手段と、
選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、
上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行できるか否かを判断する動作要件判断手段とを有し、
上記動作制御手段は、上記動作要件判断手段による判断結果に基づいて、上記ドキュメントに対する動作を制御することを特徴とする請求項１６記載の画像形成装置。
【請求項１９】
ネットワークを介して通信制御を行う通信手段と、
ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持する保持手段と、
ドキュメント属性と上記ドキュメントに対して実行される動作とに基づいて、上記保持手段によって保持される上記セキュリティポリシーを参照し、該ドキュメントへの該動作に対する上記ルールを取得するポリシー取得手段とを有し、
上記通信手段は、上記ネットワークを介して受信した上記ドキュメント属性と上記動作とを上記ポリシー取得手段に通知し、上記ポリシー取得手段が取得した上記ルールを送信することを特徴とするポリシー解釈サーバ。
【請求項２０】
上記ネットワークを介して接続される装置毎に選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、
上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ポリシー取得手段によって取得した上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行可能か否かを判断する動作要件判断手段とを有することを特徴とする請求項１９記載のポリシー解釈サーバ。

【書類名】明細書
【発明の名称】画像形成装置及びポリシー配布サーバ並びにポリシー解釈サーバ
【技術分野】
【０００１】
本発明は、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う画像形成装置に関する。
【０００２】
また、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバに関する。
【０００３】
更に、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバに関する。
【背景技術】
【０００４】
オフィスに代表されるようなドキュメントを扱うフィールドでは、そのドキュメントのセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等，特に情報のコンテナであるドキュメントに対するポリシー，中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。
【０００５】
現実に多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。
【０００６】
セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献１から、特許文献１４）。
【０００７】
例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献１）。
【０００８】
また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている(特許文献２)。
【０００９】
しかし、特に、上述の特許文献１では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。
【００１０】
また、上述の特許文献２では、セキュリティポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるＤＢ（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。
【００１１】

また、特許文献７の操作者ＩＤを入力させ、文書からＩＤを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。

【００１２】

特許文献８の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うか否かが決められているため、ルールの柔軟性に欠ける。

【００１３】

特許文献９の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【００１４】

特許文献１０の画像を読み取ってパスワードとともに記憶し,出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【００１５】

特許文献１１のネットワーク上の複数のMFPのうち、一つのMFPがユーザ管理を行ってネットワーク上のMFPすべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【００１６】

特許文献１２の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可,不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」のＩＤに対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【特許文献１】特開２００１－１８４２６４号公報
【特許文献２】特開２００１－２７３３８８号公報
【特許文献３】特開２００１－３３７８６４号公報
【特許文献４】特開平０９－２９３０３６号公報
【特許文献５】特開平０７－１４１２９６号公報
【特許文献６】特許第０２７３５９６６号公報
【特許文献７】特許３２０３１０３号公報
【特許文献８】特開平７－５８９５０号公報
【特許文献９】特開平７－１５２５２０号公報
【特許文献１０】特開平１０－１９１０７２号公報
【特許文献１１】特開２０００－１５８９８号公報
【特許文献１２】特開２０００－３５７０６４号公報
【特許文献１３】特開２００１－１２５７５９号公報
【特許文献１４】特開２００１－３２５２４９号公報。

【発明の開示】

【発明が解決しようとする課題】

【００１７】

このようなセキュリティの実施方法では、ドキュメントの印刷に対するセキュリティを実行する場合には、第１に、セキュリティの施行者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第２には、すべての機器に対してセキュリティが、一つ一つ実行される必要がある。第３には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第４に、個々の機器にセキュリティが実施されていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。

【００１８】
本発明は、上述の問題点を解決することを目的とする。
【００１９】
特に本発明の第一の目的は、ネットワークを介して外部サーバから配布されるドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて処理制御を行う画像形成装置を提供することである。
【００２０】
また、本発明の第二の目的は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバを提供することである。
【００２１】
更に、本発明の第三の目的は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバを提供することである。
【課題を解決するための手段】
【００２２】
上記第一の課題を解決するため、本発明は、請求項１に記載されるように、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有するように構成される。
【００２３】
このような画像形成装置では、外部から提供されるセキュリティポリシーで既存のセキュリティポリシーを書き換えることができる。
【００２４】
また、本発明は、請求項２に記載されるように、ネットワークを介して通信制御を行う通信手段を有し、上記ポリシー書き換え手段は、上記通信手段によって受信したセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。
【００２５】
また、本発明は、請求項３に記載されるように、上記ポリシー書き換え手段は、電源投入時に上記通信手段によって、外部から取得したセキュリティポリシーを上記ポリシー保持手段に書き込むように構成することができる。
【００２６】
また、本発明は、請求項４に記載されるように、上記ポリシー保持手段にて保持される上記セキュリティポリシーの書き換えタイミングを上記通信手段に通知するタイマー手段を有し、上記通信手段は、上記ネットワークを介して、上記セキュリティポリシーを配布するポリシー配布サーバから該セキュリティポリシーを取得するように構成することができる。
【００２７】
また、本発明は、請求項５に記載されるように、セキュリティポリシーを記憶した記憶媒体から該セキュリティポリシーを読み出すインターフェース手段を有し、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。
【００２８】
また、本発明は、請求項６に記載されるように、ネットワークを介して通信制御を行う通信手段を有し、上記通信手段は、セキュリティポリシーの選択を示す選択情報を受信すると、上記ポリシー書き換え手段に通知し、上記ポリシー書き換え手段は、上記選択情報

に基づいて、上記インターフェース手段によって読み出されたセキュリティポリシーによって、上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるように構成することができる。

【００２９】

また、本発明は、請求項７に記載されるように、上記ポリシー保持手段は、複数のセキュリティポリシーを保持し、上記ポリシー書き換え手段は、上記選択情報に基づいて、上記ポリシー保持手段で保持される上記複数のセキュリティポリシーの１つを施行すべきセキュリティポリシーとして設定するように構成することができる。

【００３０】

また、本発明は、請求項８に記載されるように、上記通信手段は、上記ネットワークを介して、Simple Object Access Protocolに従って上記セキュリティポリシーを取得するように構成することができる。

【００３１】

上記第一の課題を解決するための手段として、本発明は、上記画像形成装置での処理を行う方法、その処理コンピュータに実行させるためのプログラム、及び、そのプログラムを記憶した記憶媒体とすることもできる。

【００３２】

また、上記第二の課題を解決するために、本発明は、請求項１２に記載されるように、ネットワークを介して通信制御を行う通信手段と、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを管理するポリシー管理手段とを有し、上記通信手段は、上記ポリシー管理手段によって管理される上記セキュリティポリシーを上記ネットワークを介して接続される装置へ配布するように構成される。

【００３３】

このようなポリシー配布サーバは、ネットワークを介して接続される複数の装置に対して、同一のセキュリティポリシーを配布することができる。

【００３４】

また、本発明は、請求項１３に記載されるように、上記通信手段は、上記セキュリティポリシーを配布する際に、認証情報を同時に送信するように構成することができる。

【００３５】

また、本発明は、請求項１４に記載されるように、上記通信手段は、上記ネットワークを介して接続される上記装置から上記ポリシー管理手段によって管理される上記セキュリティポリシーの取得要求と共に、該装置の認証情報とを受信し、該認証情報に基づいた認証結果に従って、該装置へ該セキュリティポリシーを送信するように構成することができる。

【００３６】

また、本発明は、請求項１５に記載されるように、記憶媒体へ上記セキュリティポリシーを書き込むインターフェースを有し、上記ポリシー管理手段は、上記インターフェースによって、上記セキュリティポリシーを上記記憶媒体に書き込むように構成することができる。

【００３７】

また、本発明は、請求項１６に記載されるように、ドキュメントに関するドキュメント属性を、該ドキュメント属性に基づいて該ドキュメントに関する取り扱いのルールを提供する外部サーバへ送信することによって、該外部サーバから上記ルールを取得するルール取得手段と、上記ルール取得手段によって取得された上記ルールに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有するように構成される。

【００３８】

このような画像形成装置では、ドキュメントに関する取り扱いのルールをドキュメント毎及び動作毎に管理する必要がなく、また、どのルールを適用すべきかを判断する必要がない。

【００３９】

また、本発明は、請求項１７に記載されるように、上記ルール取得手段は、上記外部サーバとの通信をSimple Object Access Protocolに従って制御する通信手段を有するように構成することができる。

【００４０】

また、本発明は、請求項１８に記載されるように、上記ルール取得手段は、上記外部サーバとの通信を制御する通信手段と、選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行できるか否かを判断する動作要件判断手段とを有し、上記動作制御手段は、上記動作要件判断手段による判断結果に基づいて、上記ドキュメントに対する動作を制御するように構成することができる。

【００４１】

また、上記第三の課題を解決するために、本発明は、請求項１９に記載されるように、ネットワークを介して通信制御を行う通信手段と、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持する保持手段と、ドキュメント属性と上記ドキュメントに対して実行される動作とに基づいて、上記保持手段によって保持される上記セキュリティポリシーを参照し、該ドキュメントへの該動作に対する上記ルールを取得するポリシー取得手段とを有し、上記通信手段は、上記ネットワークを介して受信した上記ドキュメント属性と上記動作とを上記ポリシー取得手段に通知し、上記ポリシー取得手段が取得した上記ルールを送信するように構成される。

【００４２】

このようなポリシー解釈サーバでは、ドキュメントに関する取り扱いのルールをドキュメント毎及び動作毎に管理する必要がない。

【００４３】

また、本発明は、請求項２０に記載されるように、上記ネットワークを介して接続される装置毎に選択可能な機能の実行可否を示す実行可否情報を保持する選択機能保持手段と、上記選択機能保持手段によって保持される上記実行可否情報を参照することによって、上記ポリシー取得手段によって取得した上記ルールによって指定される上記動作を許可するために満たすべき動作要件を実行可能か否かを判断する動作要件判断手段とを有するように構成することができる。

【発明の効果】

【００４４】

本発明によれば、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う画像形成装置を提供することができる。

【００４５】

また、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいた処理制御を行う装置にセキュリティポリシーを配布するポリシー配布サーバを提供することができる。

【００４６】

更に、本発明は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーに基づいて、ネットワークを介して接続される装置に、該ドキュメントに対する動作を許可するための動作要件を提供するポリシー解釈サーバを提供することができる。

【発明を実施するための最良の形態】

【００４７】

以下、本発明の実施の形態を図面に基づいて説明する。

【００４８】

本発明の実施例を、以下に詳細に説明する。

【００４９】

先ず、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーについ

て説明する。

【００５０】

本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（ＤＳＰ）と呼ぶ。

【００５１】

図１は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図１のようなセキュリティポリシーを掲げることが想定される。

【００５２】

このようなポリシーをＤＳＰとして記述できるようにするために，以下のような方法を使用する。

【００５３】

まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリー（人事文書、技術関連文書など）に応じて分類する。この、機密レベルとカテゴリーの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。

【００５４】

上記のような、分類の仕方の一例を図２に示す。図２は、ドキュメントラベル用語ファイルの例を示す。図２に示されるようなドキュメントラベル用語ファイル３００は、個々のドキュメントに属性情報として付与されるラベルのリストを管理するファイルであり、例えば、ＸＭＬによって記述される。

【００５５】

ＤＳＰには、ドキュメントの機密レベル及びカテゴリーに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリーを記述するのが、図２のドキュメントラベル用語ファイル３００である。

【００５６】

図２において、<enumeration>から</enumeration>で示される記述３１１及び記述３２１によって、２種類のカテゴリーが示される。

【００５７】

記述３１１において、<enum_id>doc_category</enum_id>を示す記述３１２は、カテゴリーの識別情報が「doc_category」であることを示す。<enum_name>Document Category</enum_name>を示す記述３１３は、カテゴリーの名称が「Document Category」であることを示す。<description>文書カテゴリーの種類</description>を示す記述３１４は、このカテゴリーが何を分類するか示す説明「文書カテゴリーの種類」を示す。

【００５８】

<item>から</item>を示す記述３１５、記述３１６及び記述３１７によって、３つのカテゴリーの項目が示される。記述３１５は、<name>internal_doc</name>を示す記述によって、項目名が「internal_doc」であることを示し、<description>社内一般文書</description>を示す記述によって、その項目の説明「社内一般文書」を示す。

【００５９】

記述３１６は、<name>human_resource_doc</name>を示す記述によって、項目名が「human_resource_doc」であることを示し、<description>人事関連文書</description>を示す記述によって、その項目の説明「人事関連文書」を示す。

【００６０】

記述３１７は、<name>technical_doc</name>を示す記述によって、項目名が「technical_doc」であることを示し、<description>技術関連文書</description>を示す記述によっ

て、その項目の説明「技術関連文書」を示す。

【００６１】

同様に、記述３２１において、<enum_id>doc_security_level</enum_id>を示す記述３２２は、カテゴリーの識別情報が「doc_security_level」であることを示す。<enum_name>Document Security Level</enum_name>を示す記述３２３は、カテゴリーの名称が「Document Security Level」であることを示す。<description>文書のセキュリティレベルの種類</description>を示す記述３２４は、このカテゴリーが何を分類するか示す説明「文書のセキュリティレベルの種類」を示す。

【００６２】

<item>から</item>を示す記述３２５、記述３２６及び記述３２７によって、３つのカテゴリーの項目が示される。記述３２５は、<name>basic</name>を示す記述によって、項目名が「basic」であることを示し、<description>社外秘</description>を示す記述によって、その項目の説明「社外秘」を示す。

【００６３】

記述３２６は、<name>medium</name>を示す記述によって、項目名が「medium」であることを示し、<description>秘</description>を示す記述によって、その項目の説明「秘」を示す。

【００６４】

記述３２７は、<name>high</name>を示す記述によって、項目名が「high」であることを示し、<description>極秘</description>を示す記述によって、その項目の説明「極秘」を示す。

【００６５】

このように、ドキュメントラベル用語ファイル３００によって、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリーの種類が規定される。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が規定される。

【００６６】

図３から図１３は、ポリシー用語ファイルの例を示す図を示す。図３から図１３により、１つのポリシー用語ファイル４００を構成する。

【００６７】

図３から図１３に示されるようなポリシー用語ファイル４００は、システムタイプの分類を記述し、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。ポリシー用語ファイル４００は、例えば、ＸＭＬによって記述される。

【００６８】

図３において、列挙して記述する方法は、図２に示すドキュメントラベルファイル３００での記述方法と同様に<enumeration>から</enumeration>までの記述を繰り返すことによって示される。<enumeration>から</enumeration>までの詳細な記述は、図２に示すドキュメントラベルファイル３００での記述方法と同様であるので、ここでは、簡単な説明のみとする。

【００６９】

例えば、図３においては、記述４１１によってシステムタイプが列挙される。記述４１１によると、「システムタイプの種類」として、「複写機」、「プリンタ」、「ファクシミリ」、「スキャナ」、「文書リポジトリ」、及び、「電子会議システム」が記述される。

【００７０】

そして、例えば、図４に示されたように、記述４２１から記述４７１によってシステムタイプごとの各オペレーションが列挙される。

【００７１】

記述４２１において、「複写機に関わるオペレーション」として、「紙から紙への複写」が記述される。記述４３１において、「プリンタに係わるオペレーション」として、「

電子文書を紙へ印刷」が記載される。記述４４１において、「ファックスに関わるオペレーション」として、「ファックス送信」及び「ファックス受信」が記載される。記述４５１において、「スキャナに関わるオペレーション」として、「紙文書をスキャンして電子文書にする」が記載される。

【００７２】

記述４６１において、「文書リポジトリに関わるオペレーション」として、「保存する」、「改訂・編集する」、「削除・破棄する」、「参照する」、「ネットワークで配布する（送信する）」、「ディスクで配布する（送付する）」、及び、「アーカイブ・バックアップする」が記述される。記述４７１において、「電子会議システムに関わるオペレーション」として、「会議で利用する」が記述される。

【００７３】

更に、例えば、図６から図１３示すように、記述４８１から記述６０１によってオペレーション毎に適用できる要件が列挙される。

【００７４】

記述４８１において、「複写に関わる要件」として、「明示的な許可」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【００７５】

記述４９１において、「印刷に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「プリントした本人による紙出力」、「信頼チャネルの利用（印刷データの暗号化）」、及び、「プリントアウトに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【００７６】

記述５０１において、「ファックス送信に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「宛先制限」、「親展モードでの送信」、「信頼チャネルの利用」、「送信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」、及び、「否認防止（受取証の取得）」が記載される。

【００７７】

記述５１１において、「ファックス受信に関わる要件」として、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「親展ファックスの宛先本人による取り出し」、「信頼タイムスタンプ」、及び、「受信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【００７８】

記述５２１において、「スキャンに関わる要件（保存した後については保存要件を適用する）」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「スキャン画像に追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【００７９】

記述５３１において、「保存に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「保存データの暗号化」、及び、「保存データの改ざん保護」が記載される。

【００８０】

記述５４１において、「改訂に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「バージョン管理」が記載される。

【００８１】

記述５５１において、「削除・破棄に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「完全消去」が記載される。

【００８２】

記述５６１において、「参照に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「編集禁止のデータのみ参照許可」、「印刷禁止のデータのみ参照

許可」、「参照場所限定のデータのみ参照許可」、及び、「ユーザ限定のデータのみ参照許可」が記載される。

【００８３】

記述５７１において、「ネットワーク配信（送信）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「信頼チャネルの利用（送信データの暗号化）」、「宛先制限（社内のみ配信可能など）」、「編集禁止のデータのみ配信許可」、「印刷禁止のみ配信許可」、「参照場所限定のデータのみ配信許可」、及び、「ユーザ限定のデータのみ配信許可」が記載される。

【００８４】

記述５８１において、「ディスク配布（送付）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「送付データの暗号化」、「送付データの改ざん保護」、「編集禁止のデータのみ送付許可」、「印刷禁止のみ送付許可」、「参照場所限定のデータのみ送付許可」、及び、「ユーザ限定のデータのみ送付許可」が記載される。

【００８５】

記述５９１において、「アーカイブ・バックアップに関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「アーカイブデータの暗号化」、及び、「アーカイブデータの改ざん保護」が記載される。

【００８６】

記述６０１において、「会議での利用に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【００８７】

図２のドキュメントラベル用語ファイルと図３から図１３のポリシー用語ファイルとに基づくＤＳＰについて図１４から図２２で説明する。図１４から図２２は、ポリシーファイルの例を示す図である。上述の図２に示すドキュメントラベル用語ファイル３００と、図３から図１３のポリシー用語ファイル４００とに基づいて、ユーザの組織内でのセキュリティに対するポリシーが、例えば図１４から図２２に示すＤＳＰ２０００のようにＸＭＬで記述され、１つのポリシーファイルを構成する。

【００８８】

図１４から図２２に示されるようなＤＳＰ２０００は、<policy>で示される記述２００１から</policy>で示される記述２００２にてポリシーが示される。

【００８９】

図１４の<acc_rule>を示す記述２０１１から図１６の</acc_rule>を示す記述２０１２において、<doc_category>ANY</doc_category>及び<doc_security_level>basic</doc_security_level>を示す記述２０１３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「basic（基本レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０１７によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００９０】

図１６の<acc_rule>を示す記述２０２１から図１９の</acc_rule>を示す記述２０２２において、<doc_category>ANY</doc_category>及び<doc_security_level>medium</doc_security_level>を示す記述２０２３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「medium（中レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０２７によって、ユーザカテゴ

リ「DOC-CATEGORY（文書カテゴリーの種類）」（図２の記述３１２、３１３及び３１４参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００９１】

また、同様のドキュメント属性を有するドキュメントに対して、図１８の<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０２８によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００９２】

図１９の<acc_rule>を示す記述２０３１から図１９の</acc_rule>を示す記述２０３２において、<doc_category>ANY</doc_category>及び<doc_security_level>high</doc_security_level>を示す記述２０２３によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「high（高レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述２０３７によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリーの種類）」（図２の記述３１２、３１３及び３１４参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【００９３】

次に、図１４から図２２のＤＳＰ２０００の構造を、図２３から図２５を参照して、以下に、詳しく説明する。

【００９４】

図２３は、ＤＳＰの識別情報の例を示す図である。ＤＳＰ２０００の識別情報２１０において、＜about_this_policy＞と＜/about_this_policy＞とで囲まれた範囲の記述２１１～２１３には、ＤＳＰ２０００を識別するための識別情報が記述される。

【００９５】

<serial_number>RDSP2023</serial_number>を示す記述２１１には、ＤＳＰ２０００を他のＤＳＰと区別するためのシリアル番号が記述される。

【００９６】

<terminology_applied>RDST9487</terminology_applied>で示される記述２１２には、ＤＳＰ２０００に対応するポリシー用語ファイル４００のシリアル番号が記述される。尚、この定義ファイルは更新される可能性があるため、このＤＳＰ２０００がどのポリシー用語ファイルに基づいて記述されているのかを明確にするために記録しておく。記述２１３には、<title> DOCUMENT-SECURITY-POLICY</title>を示す記述によってＤＳＰ２０００のタイトル、<version>1.20</version>を示す記述によってバージョン番号、<creation_date>2002/02/18 22:30:24</creation_date>を示す記述によって作成日時、<creator>Taro Tokyo</creator>を示す記述によって作成者、<description>sample document security policy.</description>を示す記述によって説明などの一般的な書誌情報が記述される。

【００９７】

そして、ＤＳＰ２０００の識別情報は、</about_this_policy>により終了する。

【００９８】

次に、上述のＤＳＰ２００の識別情報に続いて、ポリシーの内容を<policy>と</policy>で囲まれた範囲に記述する。図２４は、ＤＳＰの構造を説明するための記述例を示す図である。

【００９９】

図２４に示されるポリシーの内容２２０は、以下に説明するように、階層構造を用いて記録する。

【０１００】

ポリシー<policy>は、複数のアクセス制御ルール<acc_rule>（記述２２１）で構成される。一つのアクセス制御ルール<acc_rule>（記述２２１）は、対象とするドキュメントのカテゴリー<doc_category>とレベル<doc_security_level>を一意に指定し（記述２２２），さらにアクセス制御リスト<acl>（記述２２３）を一つ含むように構成される。

【０１０１】

アクセス制御リスト<acl>（記述２２３）は、複数のアクセス制御エレメント<ace>（記述２２４）で構成される。

【０１０２】

各アクセス制御エレメント<ace>（記述２２４）は、対象とするユーザのカテゴリー<user_category>（記述２２５）とレベル<user_security_level>（記述２２６）を一意に指定し，さらに複数のオペレーション<operation>（記述２２７）で構成される。

【０１０３】

各<operation>（記述２２７）は、一つのオペレーション名<name>（記述２２８）と、一つの禁止<denied/>（記述２２９）、または一つの許可<allowed/>（記述２３２）、または複数の<requirement>（記述２３０及び記述２３１）で構成される。

【０１０４】

記述２２２において、ドキュメントのカテゴリー<doc_category>やユーザのカテゴリー<user_category_level>に記述している”ANY”は、どのカテゴリー、及び、レベルにも適用されることを示している。また、記述２２５によって示されるユーザのカテゴリー<user_category>の”DOC-CATEGORY”は、ユーザのカテゴリーがドキュメントのカテゴリーと同じときに適用されることを示している。

【０１０５】

この実施例では、禁止するオペレーションには<denied/>（記述２２９）を指定するようにしているが、ＤＳＰ２０００に記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【０１０６】

このように、ＤＳＰを記述することにより、ドキュメントのタイプ（カテゴリー、レベル）に応じて，どのようなユーザタイプ（カテゴリー、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能な場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【０１０７】

そして、ＤＳＰを、上記のようにプラットフォームに依存しないXMLで記述することにより、異なるタイプのシステム間で、このＤＳＰを共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図３から図１３のドキュメントラベルファイルや図１４から図２２のＤＳＰ２０００に記述しているように、紙ドキュメントに関するオペレーション（hardcopy，scanなど）も規定できる。

【０１０８】

本実施例の、図２４に示す要件の中に、以下の<requirement>explicit_authorization</requirement>を示す記述２３１が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、このＤＳＰに従ってオペレーションがコントロールされるようになると、自由

度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【０１０９】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと，明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【０１１０】

従って、ＤＳＰに記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまってオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【０１１１】

次に本発明のＤＳＰの別の記述形を図２６で説明する。図２５は、ＤＳＰの他の記述例を示す図である。図２６に示すポリシーの内容２４０は、無条件で許可するオペレーションや、禁止するオペレーションが多くなった場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>を示す記述２４３と、許可しないオペレーションを列挙する、<denied_operations>を示す記述２４１を使用するようにしても良い。

【０１１２】

また、<requirement>explicit_authorization</requirement>を示す記述２４２は、図２４での説明と同様である。

【０１１３】

図２６は、上述のＤＳＰを蓄積し且つ配布する種々の媒体を示す。

【０１１４】

以上で説明したように、図２６に示されたＤＳＰ２０００は、XML（Ｅｘｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ、ＤＶＤ－Ｒ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ、ＤＶＤ＋Ｒのような光ディスク５４のような記憶媒体を作成することができる。また、その電子的なＤＳＰ２０００をコンピュータ５５を使用して、ネットワーク５６を介してで伝送することができる。

【０１１５】

このＤＳＰ２０００は、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従って、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【０１１６】

図２７は、本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。図２７において、画像形成装置１０００は、コンピュータによって制御される装置であって、ＣＰＵ（中央処理装置）１１と、ＲＯＭ（Read-Only Memory）１２と、ＲＡＭ（Random Access Memory）１３と、不揮発性ＲＡＭ（non-volatile Random Access Memory）１４と、リアルタイムクロック１５、イーサネット（登録商標）Ｉ／Ｆ（Ethernet（登録商標） Interface）２１と、ＵＳＢ（Universal Serial Bus）２２と、ＩＥＥＥ（Institute of Electrical and Electronics Engineers）1284 ２３と、ハードディスクＩ／Ｆ２４と、エンジンＩ／Ｆ２５と、ＲＳ－２３２Ｃ　Ｉ／Ｆ２６と、ドライバ２７とで

構成され、システムバスＢに接続される。

【０１１７】

ＣＰＵ１１は、ＲＯＭ１２に格納されたプログラムに従って画像形成装置１０００を制御する。ＲＡＭ１３には、例えば、各インターフェース２１から２６に接続される資源に領域が割り当てられる。不揮発性ＲＡＭ１４には、画像形成装置１０００を制御するためにＣＰＵ１１による処理で必要な情報が格納される。リアルタイムクロック１５は、現時刻を計ると共に、処理を同期させる場合にＣＰＵ１１によって使用される。

【０１１８】

イーサネット（登録商標）Ｉ／Ｆ２１には、１０ＢＡＳＥ－Ｔ又は１００ＢＡＳＥ－ＴＸ等のイーサネット（登録商標）用インターフェースケーブルが接続される。ＵＳＢ２２には、ＵＳＢ用インターフェースケーブルが接続される。ＩＥＥＥ1284 ２３には、ＩＥＥＥ1284用インターフェースケーブルが接続される。

【０１１９】

ハードディスクＩ／Ｆ２４には、ハードディスク３４が接続され、ネットワークを介して送信された印刷すべき文書の文書データ、又は、印刷処理後の画像データがハードディスクＩ／Ｆ２４を介してハードディスク３４に格納される。エンジンＩ／Ｆ２５には、文書データに基づいて所定媒体に印刷を行うプロッタ３５－１及び画像データを取り込むスキャナ３５－２等が接続される。ＲＳ－２３２Ｃ　Ｉ／Ｆ２６には、オペレーションパネル３６が接続され、ユーザへの情報の表示及びユーザから入力情報又は設定情報の取得が行われる。

【０１２０】

画像形成装置１０００によって行われる処理を実現するプログラムは、例えば、ＣＤ－ＲＯＭ等の記憶媒体３７によって画像形成装置１０００に提供される。即ち、プログラムが保存された記憶媒体３７がドライバ２７にセットされると、ドライバ２７が記憶媒体３７からプログラムを読み出し、その読み出されたプログラムがシステムバスＢを介してハードディスク３４にインストールされる。そして、プログラムが起動されると、ハードディスク３４にインストールされたプログラムに従ってＣＰＵ１１がその処理を開始する。尚、プログラムを格納する記憶媒体３７としてＣＤ－ＲＯＭに限定するものではなく、コンピュータが読み取り可能な記憶媒体であればよい。プログラムをネットワークを介してダウンロードし、ハードディスク３４にインストールするようにしても良い。

【０１２１】

セキュリティポリシーに従って動作する画像形成装置について図２８、図２９及び図３０を参照して以下に詳細に説明する。

【０１２２】

図２８は、セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。

【０１２３】

図２８に示す読み取り装置としての画像形成装置１０００は、主に、読み取り部７１と、読み取り条件取得部７２と、データ送信先取得部７３と、データ処理部７４と、データ送信部７５と、ポリシー実行部１００１と、読み取り画像データ６１と、蓄積データ６２とを有する。

【０１２４】

また、ポリシー実行部１００１は、ドキュメント属性取得部１０１１と、動作要件選択部１０１２と、動作制御部１０１３と、ユーザ属性取得部１０２１とを有する。ドキュメント属性取得部１０１１は紙原稿６０から又は読み取り画像データ６１からドキュメント属性を取得して、動作要件選択部１０２１へ通知する。

【０１２５】

一方、ユーザ属性取得部１０２１は、ユーザによって入力されたユーザ情報を取得すると、動作要件選択部１０１２に通知する。動作要件選択部１０１２は、ＤＳＰ２０００に従って許可される場合の要件を選択し、その結果を動作制御部１０１３に通知する。動作

制御部１０１３は、読み取った紙原稿６０の画像データに対するデータ処理を指示する。

【０１２６】

ポリシー実行部１００１において、点線で示される部分について省略しても良い。

【０１２７】

読み取り部７１は、読み取り条件取得部７２から通知されるユーザによって入力された読み取り条件に従って、紙原稿６０を読み取る（スキャン）する処理部であり、読み取った画像データは、読み取り画像データ６１に格納される。また、画像データ６１から取得したドキュメント属性をドキュメント属性取得部１０１１に通知する。

【０１２８】

読み取り条件取得部７２は、ユーザによって入力された読み取り条件を取得し、読み取り部７１とデータ処理部７４とへ通知する。

【０１２９】

データ送信先取得部７３は、ユーザによって入力されたデータ送信先を取得し、データ送信部７５に通知する処理部である。

【０１３０】

データ処理部７４は、動作制御部１０１３から提供される要件を満たすように読み取り条件取得部７２から通知されるユーザによって入力された読み取り条件に従って、データ処理を読み取った画像データに行い、データ処理された画像データを蓄積データ６２に蓄積する。

【０１３１】

データ送信部７５は、動作制御部１０１３から通知される要件を満たすように、蓄積データ６２から取り出した処理対象となる画像データをデータ送信先取得部７３から通知された送信先へ送信する。

【０１３２】

画像データを外部に送信する必要がない場合、データ送信部２８を省略しても良い。また、画像データを記憶媒体３７に記憶するようにしても良い。

【０１３３】

図２８において、読み取り装置としての画像形成装置１０００は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。

【０１３４】

また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記憶媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【０１３５】

図２９は、簡略化したＤＳＰの例を示す図である。説明の便宜のため、ＤＳＰ２０００を簡略化したＤＳＰで説明する。図２９に示されるＤＳＰ２１００において、つぎのようにルール１からルール３を示す。

【０１３６】

ルール１は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１１行目<operation>から、第１４行目</operation>までの部分により記述される。

【０１３７】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール１が適用されることを示す。

【０１３８】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１３９】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないこととを示す。

【０１４０】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１４１】

更に第１２行目と第１３行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【０１４２】

従って、ルール１では、第５行目、第６行目、第９行目、第１０行目、第１２行目及び第１３行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは要件なく許可される。

【０１４３】

次に、ルール２は、図２９の第４行目の<acc_rule>から、第１０行目の<user_security_level>ANY</user_security_level>までの部分及び、第１５行目<operation>から、第２０行目</operation>までの部分により記述される。

【０１４４】

第５行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわりなくルール２が適用されることを示している。

【０１４５】

第６行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【０１４６】

第９行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【０１４７】

第１０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１４８】

更に、第１６行目から第１９行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【０１４９】

従って、ルール２では、第５行目、第６行目、第９行目、第１０行目、第１６行目から第１９行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”basic”の場合には、ユーザのカテゴリーにかかわりなく、且つ、ユーザのセキュリティレベルにかかわりなく、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【０１５０】

そして、ルール３は、図２９の第２４行目の<acc_rule>から、第３０行目の<user_security_level>ANY</user_security_level>までの部分及び、第３１行目<operation>から、第３５行目</operation>までの部分により記述される。

【０１５１】

第２５行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわりないこ

とを示す。

【０１５２】

第２６行目の<doc_security_level>high</doc_security_level>は、文書のセキュリティレベルがhighの場合を示す。

【０１５３】

第２９行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【０１５４】

第３０行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【０１５５】

第３２行目から第３４行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【０１５６】

従って、ルール３では、第２５行目、第２６行目、第２９行目、第３０行目、第３１行目から第３４行目により、文書カテゴリーにかかわりなく、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわりなく、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【０１５７】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【０１５８】

図２８を参照しつつ、詳細な動作について説明する。

【０１５９】

上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【０１６０】

また、上述の図２９に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【０１６１】

次に、セキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、動作制御部１０１３は、データ処理部７１に対して、文書の読み取りを指示し、ユーザは文書データを取得して終了する。

【０１６２】

一方、セキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場

合には、動作要件選択部１０１２は、その要件をすべて満たすことができるかを判定し、その判断結果を動作制御部１０１３に通知する。

【０１６３】

動作要件選択部１０１２による判断結果がすべての要件を満たすことができないことを示す場合は、動作制御部１０１３は、データ処理部７４に対してデータ処理を禁止するように指示し、データ処理部７４は読み取りデータを破棄して終了する。ユーザに対してはデータ処理が行えないことを通知する。

【０１６４】

一方、動作要件選択部１０１２による判断結果がすべての要件を満たすことができることを示す場合は、動作制御部１０１３データ処理部７４に対して、その要件を満たすようにデータ処理を行うように指示する。ユーザは文書データを取得して終了する。

【０１６５】

この場合には、以下の処理が実行される。

【０１６６】

ユーザ属性取得部１０２１は、オペレーションパネル３６から読み取り指示を出したユーザに、ユーザＩＤの入力要求を出す。ユーザは、オペレーションパネル３６からユーザＩＤを入力する。ユーザ属性取得部１０２１は、ユーザＩＤからデータベース１０２に登録されている入力されたユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部１０２１に通知する。

【０１６７】

ログを記録する場合、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【０１６８】

最後に、ユーザは紙原稿６０の画像データを蓄積データ６２内に取得して終了する。

【０１６９】

以上のように、図２９に示したセキュリティポリシーに従って、紙原稿（ドキュメント）６０を読み取ることができる。

【０１７０】

次に、画像形成装置１０００が紙原稿６０を読み取り且つ読み取った文書をネットワークに配信する場合について説明する。

【０１７１】

先ず、ユーザが、画像形成装置１０００に紙原稿６０をセットし、オペレーションパネル３６から、読み取り条件の入力、読み取りデータの配信先の指定及び紙原稿６０の読み取り指示を出す。

【０１７２】

読み取り部７１が、紙文書の読み取りを行う。ドキュメント属性取得部１０１１は、読み取った紙原稿６０の画像データのバーコードや電子透かしなどの画像情報から文書ＩＤを抽出し、カテゴリー、セキュリティレベルを取得して、動作要件選択部１０１２に通知する。

【０１７３】

動作要件選択部１０１２は、ドキュメント属性取得部１０１１が通知したドキュメント属性に従って、ＤＳＰ２１００の中の対応するエントリを検索し、要件を抽出する。

【０１７４】

上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【０１７５】
また、上述の図２９に示すＤＳＰ２１００に基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【０１７６】
例えば、ドキュメントをネットワークへ配信する際の要件が、ＤＳＰ２１００内に存在しない場合には、動作制御部１０１３は、データ送信部７５に対して配信の指示を行い、ドキュメントをネットワークへ配信して、処理を終了する。

【０１７７】
一方、例えば、ドキュメントをネットワークへ配信する際の要件が、ＤＳＰ２１００内に存在する場合には、動作要件選択部１０１２が、その要件をすべて満たすことができるかを判定する。

【０１７８】
ネットワークに配信することを許可するルールがない場合には、動作制御部１０１３が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、紙原稿６０の画像データを破棄して終了する。例えば、セキュリティレベルが”high”の場合である。

【０１７９】
動作要件選択部１０１２によってすべての要件を満たすことができないと判断した場合は、動作制御部１０１３が、ユーザに通知をして、データ処理部７４に対して紙原稿６０の画像データを破棄するように指示して終了する。

【０１８０】
例えば、上述のセキュリティレベルが”basic”の場合のように、すべての要件を満たすことができる場合は、動作制御部１０１３は、その要件を満たした読み取りをデータ処理部７４に指示し、また、データ送信部７５にドキュメントをネットワークに配信するように指示して終了する。

【０１８１】
そして、ユーザ属性取得部１０１２は、オペレーションパネル３６から読み取り指示を出したユーザに、ユーザＩＤの入力要求を出す。

【０１８２】
ユーザが、オペレーションパネル３６からユーザＩＤを入力すると、ユーザ属性取得部１０２１は、ユーザＩＤに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部１０１２に通知する。動作制御部１０１３は、動作要件選択部１０１２から通知される要件に従ってログを記録する。

【０１８３】
更に、動作制御部１０１３は、データ処理部７４に対して、読み取った紙原稿６０の画像データを、印刷不可能なデータ(たとえばADOBE（登録商標）の印刷禁止属性を持ったPDFなど)に変換するように指示を行う。

【０１８４】
最後に、動作制御部１０１３は、データ送信部７５に対して配信指示を行い、データ送信部７５は、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、ドキュメントをネットワークへ配信し、終了する。

【０１８５】
以上のように、図２９に示したＤＳＰ２１００を使用して、図２８に示した文書読み取り装置としての画像形成装置１０００が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【０１８６】

セキュリティポリシーに従った動作を実現する複写装置としての画像形成装置の機能構成について図３０で説明する。図３０は、セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。図３０中、図２８と同様の処理部には同一符号を付しその詳細な説明を省略する。

【０１８７】

図３０において、複写装置としての画像形成装置１０００－２は、図２８に示す画像形成装置１０００の読み取り条件取得部７２及びデータ送信先取得部７３の代わりに複写条件取得部８１と、図２８に示す画像形成装置１０００のデータ送信部７５の代わりに印刷部８２とを有する点において、図２８に示す画像形成装置１０００と異なっている。

【０１８８】

しかしながら、画像形成装置１０００が画像形成装置１０００－２の複写条件取得部８１と、印刷部８２とを更に有するように構成しても良い。点線で示される部分１００２は省略しても良い。

【０１８９】

複写条件取得部８１は、ユーザがオペレーションパネル３６に入力した複写条件を取得して、読み取り部７１とデータ処理部７４とへ複写条件を通知すると共に、印刷部８２へも通知する。

【０１９０】

印刷部８２は、動作制御部１０１３からの指示に応じて、蓄積データ６２から紙原稿６０の画像データを取得し、動作制御部１０１３から通知された要件を満たすように複写条件取得部８１から通知されて複写条件に従って印刷処理を行い、用紙に画像データが形成された複写原稿６０ｂを出力する。

【０１９１】

以下に、外部から画像形成装置１０００又は１０００－２に対してポリシーを設定する方法について説明する。例えば、ポリシーとして図１４から図２２に記載されるＤＳＰ２０００が配布される。ポリシーとしてＤＳＰ２０００が、外部サーバから画像形成装置１０００又は１０００－２へ配布される際には、ＳＯＡＰ(Simple Object Access Protocol)に従った通信によって行われる。

【０１９２】

図３１から図４４に示される画像形成装置１０００又は１０００－２は、読み取り装置又は複写装置としての画像形成装置に限定されず、読み取り機能と複写機能とを有する、或いは、それ以上の（例えば、スキャナ、コピー、ＦＡＸ、プリンタ等）複数の異なる画像形成処理を可能とする画像形成装置であっても良い。

【０１９３】

先ず、画像形成装置１０００又は１０００－２が一方的に送り付けられるポリシーを受信する第一のポリシー設定方法について図３１で説明する。

【０１９４】

図３１は、外部サーバからポリシーが配布される第一のポリシー設定方法を示す図である。図３１において、ポリシーを設定しようとする管理者が使用する管理者コンソール４００１と、外部サーバとしてポリシーを配布するポリシー配布サーバ４０００と、画像形成装置１０００又は１０００－２とがネットワーク５を介して接続される。ポリシー配布サーバ４０００は、サーバコンピュータであって、ＳＯＡＰクライアント機能４０２１を有し、画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２を有する。図３１中、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０１９５】

図３１に示す第一のポリシー設定方法では、管理者が管理者コンソール４００１からポリシーとしてＤＳＰ２０００をポリシー配布サーバ４０００に送信する（ステップＳ１１）。そして、ポリシー配布サーバ４０００がＳＯＡＰクライアント機能４０２１を利用して、ポリシーとしてＤＳＰ２０００を配布し（ステップＳ１２）、画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２でＤＳＰ２０００をポリシーとして受信し、受信結果を

返す。

【０１９６】

そして、画像形成装置１０００は、配布されたＤＳＰ２０００に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップＳ１３）。

【０１９７】

このような構成の場合に、画像形成装置１０００は、ポリシーを送信するポリシー配布サーバ４０００が信頼できるものであるか否かを確かめることで、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。すなわち、ポリシー配布サーバ４０００がポリシーの配布をする時に、以下のような動作を実行する。

【０１９８】

上記ステップＳ１２において、ポリシー配布サーバ４０００は、自分自身の認証情報とポリシーとしてＤＳＰ２０００を画像形成装置１０００に送信する。

【０１９９】

次に、画像形成装置１０００は、送信されたポリシー配布サーバ４０００の認証情報を検証する（ステップＳ１２－２）。

【０２００】

そして、このポリシー配布サービス４０００の認証情報が正しいと確認された場合、画像形成装置１０００は、ポリシーとして送信されたＤＳＰ２０００を正式なものと見なして、配布されたＤＳＰ２０００に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップＳ１３）。

【０２０１】

このようなポリシー配布サーバ４０００の認証を行うことによって、画像形成装置１０００は、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐことができる。

【０２０２】

次に、画像形成装置１０００又は１０００－２が、ポリシー配布サーバ４０００からポリシーの配布通知を受けてポリシーを取得しにいく第二のポリシー設定方法について図３２で説明する。

【０２０３】

図３２は、外部サーバからポリシーを取得する第二のポリシー設定方法を示す図である。図３２において、図３１と同様に、管理者コンソール４００１と、ポリシー配布サーバ４０００と、画像形成装置１０００又は１０００－２とがネットワーク５を介して接続される。ポリシー配布サーバ４０００は、ＳＯＡＰクライアント機能４０２１とＳＯＡＰサーバ機能２０２４とを有し、画像形成装置１０００又は１０００－２は、ＳＯＡＰサーバ機能４０２２とＳＯＡＰクライアント機能４０２３とを有する。図３２中、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０２０４】

図３２に示す第二のポリシー設定方法では、管理者が管理者コンソール４００１からポリシーとしてＤＳＰ２０００をポリシー配布サーバ４０００に送信する（ステップＳ２１）。そして、ポリシー配布サーバ４０００がＳＯＡＰクライアント機能４０２０を利用して、ポリシーとしてＤＳＰ２０００の配布があったことを通知し（ステップＳ２２）、画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２でその配布通知を受信し、受信結果を返す。

【０２０５】

その後、画像形成装置１０００は、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー取得要求を送信すると、ポリシー配布サーバ４０００は、ＳＯＡＰサーバ機能２０２４でそのポリシー取得要求を受信して、受信結果としてポリシー（管理者コンソール４００１から受信したＤＳＰ２０００）を送信する（ステップＳ２３）。

【０２０６】

そして、画像形成装置１０００は、配布されたＤＳＰ２０００に従って、動作要件の選択を行い、動作要件を満たすように動作する（ステップＳ２４）。

【０２０７】
ステップＳ２２にて、ポリシー配布サーバ４０００は、画像形成装置１０００にＤＳＰ２０００を識別する識別情報を送信することによってポリシー配布通知を行うようにしても良い。この場合、ステップＳ２３において、画像形成装置１０００は、ポリシー配布サーバ４０００から受信した識別情報を送信することによってポリシー取得要求を行うようにすれば良い。
【０２０８】
更に、このような場合には、ポリシーを受信する画像形成装置１０００が信頼できるものであるか否かを確かめることで情報の漏洩（ここではポリシー）を防ぐことができる。即ち、画像形成装置がポリシー配布サーバ４０００からポリシーを取得する際に以下のような動作を実行する。
【０２０９】
先ず、上記ステップＳ２３において、画像形成装置１０００は、自分自身の認証情報をポリシー取得要求に付加して、ポリシー配布サーバ４０００に送信する。
【０２１０】
次に、ポリシー配布サーバ４０００は、画像形成装置１０００から受信した認証情報を検証する（ステップＳ２３－２）。そして、ポリシー配布サーバ４０００は、画像形成装置１０００の認証情報が正しいと確認した場合、ポリシーとしてＤＳＰ２０００を画像形成装置１０００へ送信する（ステップＳ２３－４）。
【０２１１】
このような画像形成装置１０００の認証を行うことによって、ポリシー配布サーバ４０００は、情報の漏洩（ここではポリシー）を防ぐことができる。
【０２１２】
第二のポリシー設定方法は、画像形成装置１０００が比較的容量のあるポリシーを次々に受信すると記憶領域が不足してしまうような場合に、画像形成装置１０００が必要な時にポリシーを取得するようにすることができる点で有効である。
【０２１３】
この第二のポリシー設定方法において、画像形成装置１０００は、配布通知を受けて速やかにポリシー取得要求を行っても良いし、配布通知を受けたことを装置内部に記憶しておいて、所定のタイミングでポリシー取得要求を行っても良い。
【０２１４】
所定のタイミングでポリシー取得要求を行うポリシー設定方法の変形例について図３３、図３４及び図３５について説明する。
【０２１５】
図３３は、電源投入時にポリシーを取得する第三のポリシー設定方法を示す図である。図３３中、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。図３３に示す第三のポリシー設定方法は、画像形成装置１０００が最初にネットワーク５に接続した場合などのように、まだセキュリティポリシーを持っていない場合のポリシー設定方法である。
【０２１６】
図３３において、画像形成装置１０００に電源投入されると（ステップＳ３１）、ネットワーク５を介して、ポリシー配布サーバ４０００に対して、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー取得要求を行う（ステップＳ３２）。ポリシー配布サーバ４０００は、ＳＯＡＰサーバ機能を利用して、ポリシー取得要求を受信し、ポリシー（管理者コンソール４００１から受信したＤＳＰ２０００）を受信結果として送信する。
【０２１７】
画像形成装置１０００は、ポリシー配布サーバ４０００からポリシーを受信すると、動作要件を満たすように動作する（ステップＳ３３）。
【０２１８】
図３４は、電源投入時にポリシーを取得する第四のポリシー設定方法を示す図である。

図３４中、図３３と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。図３４において、ポリシー配布サーバ４０００は、更に、識別情報比較部４０２９を有することである。

【０２１９】

画像形成装置１０００に電源投入されると（ステップＳ４１）、ネットワーク５を介して、ポリシー配布サーバ４０００に対して、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー取得要求を行うと同時に、現在のＤＳＰ２０００の識別情報（例えば、図２３の記述２１１で示される「ＲＤＳＰ２０２３」）を同時に送信する（ステップＳ４２）。

【０２２０】

ポリシー配布サーバ４０００は、ＳＯＡＰサーバ機能を利用して、ポリシー取得要求を受信すると、識別情報比較部４０２９によって、受信した識別情報（例えば、「ＲＤＳＰ２０２３」）と、配布するポリシーの識別情報とを比較する（ステップＳ４３）。同じ場合は、同じ識別情報であるという受信結果だけを送信するようにする。同じでない場合に、ポリシー配布サーバ４０００は画像形成装置１０００に対して、受信結果としてポリシー（管理者コンソール４００１から受信したＤＳＰ２０００）を送信する（ステップＳ４４）。

【０２２１】

画像形成装置１０００は、ポリシー配布サーバ４０００からポリシーを受信すると、受信したポリシーで保持していたポリシーを書き換えて、ポリシーに従って動作要件の選択を行い、動作要件を満たすように動作する（ステップＳ４５）。

【０２２２】

この第二の変形例では、識別情報が同一である場合、ポリシーを配布しないため、無駄なトラフィックを軽減することができる。

【０２２３】

図３５は、電源投入時にポリシーを取得する第五のポリシー設定方法を示す図である。図３５中、図３３と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０２２４】

画像形成装置１０００に電源投入されると（ステップＳ５１）、ネットワーク５を介して、ポリシー配布サーバ４０００に対して、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー配布要求を行う（ステップＳ５２）。ポリシー配布サーバ４０００は、ＳＯＡＰサーバ機能４０２４によってポリシー配布要求を受信すると、受信結果を画像形成装置１０００に送信する。

【０２２５】

その後、ポリシー配布サーバ４０００は、ＳＯＡＰクライアント機能４０２１によって、ポリシーを送信し、画像形成装置１０００がそのポリシーを受信して、受信結果をポリシー配布サーバ４０００へ返す（ステップＳ５３）。

【０２２６】

画像形成装置１０００は、ポリシー配布サーバ４０００からポリシーを受信すると、ポリシーに従って動作要件の選択を行い、動作要件を満たすように動作する（ステップＳ５４）。

【０２２７】

この第五のポリシー設定方法において、ポリシー配布サーバ４０００は、画像形成装置１０００からポリシー取得要求を受けた後速やかにポリシーを配布しても良いし、ポリシー取得要求を受けたことをポリシー配布サーバ４０００の内部に記憶しておいて、所定のタイミングでポリシーを配布するようにしても良い。

【０２２８】

また、この第五のポリシー設定方法において、図３４に示す第四のポリシー設定方法の

ように、ポリシー配布サーバ４０００に識別情報比較部４０２９を備える構成としても良い。このような構成とすることによって、無駄なトラヒックを軽減することができる。

【０２２９】

図３１から図３６にて説明した第一及び第五のポリシー設定方法を実現するための機能構成について図３６で説明する。図３６は、第一から第五のポリシー設定方法を実現するための機能構成の例を示す図である。図３６における説明において、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２３０】

図３６において、画像形成装置１０００の動作要件選択部１０１２は、ポリシー解釈部４１０１と、選択要件検証部４１０２と、通信部４１０３と、ポリシー書き換え部４１０４と、ＤＳＰ２０００ａと、システム属性９１ａとを有する。

【０２３１】

ポリシー解釈部４１０１は、ドキュメント属性取得部１０１１によって取得されたドキュメント属性と、ユーザ属性取得部１０２１によって取得されたユーザ属性とに対するポリシーを、ＤＳＰ２０００ａに基づいて解釈する。そして、ポリシー解釈部４１０１は、その解釈結果として動作要件を選択要件検証部４１０２に通知する。つまり、ユーザが指定する動作を実行する際に満たさなければならない動作要件が通知される。

【０２３２】

選択要件検証部４１０２は、システム属性９１ａを参照することによって、ポリシー解釈部４１０１から通知された動作要件を満たすことができるか否かを判断する。そして、選択要件検証部４１０２は、その判断結果を動作制御部１０１３へ通知する。

【０２３３】

通信部４１０３は、ＳＯＡＰに従ってポリシー配布サーバ４０００との通信を制御する処理部であり、図３１から図３５に示すＳＯＡＰサーバ機能４０２２及びＳＯＡＰクライアント機能４０２３の少なくとも１つ以上を備えている。通信部４１０３は、ポリシー配布サーバ４０００からポリシーとしてＤＳＰ２０００ｂを受信すると、ポリシー書き換え部４１０４に通知する。また、図３２に示すように、ポリシー配布サーバ４０００に対して、ポリシー取得要求を行う際には、画像形成装置１０００を認証するための認証情報を同時に送信する。

【０２３４】

ポリシー書き換え部４１０４は、受信したＤＳＰ２０００ｂでＤＳＰ２０００ａを書き換える。また、ポリシー書き換え部４１０４は、図３１に示されるように、認証情報がＤＳＰ２０００ｂと同時に配布された場合、その認証情報に基づいてポリシー配布サーバ４０００を認証し、ポリシー配布サーバ４０００が認証された場合のみ、受信したＤＳＰ２０００ｂでＤＳＰ２０００ａを書き換える。

【０２３５】

ポリシー配布サーバ４０００は、通信部４１２３と、ポリシー管理部４１２４と、ＤＳＰ２０００ｂとを有する。

【０２３６】

通信部４１２３は、ＳＯＡＰに従って画像形成装置１０００との通信を制御する処理部であり、図３１から図３５に示すＳＯＡＰサーバ機能４０２１及びＳＯＡＰクライアント機能４０２４の少なくとも１つ以上を備えている。通信部４１２３は、ＤＳＰ２０００ｂを配布する。

【０２３７】

ポリシー管理部４１２４は、配布するＤＳＰ２０００ｂを管理する。ポリシー管理部４１２４は、図３１に示すように、通信部４１２３によって、ＤＳＰ２０００ｂを配布する際に、ポリシー配布サーバ４０００を認証するための認証情報を同時に送信させる。また、ポリシー管理部４１２４は、ポリシー取得要求に画像形成装置１０００の認証情報が同

時に送信された場合、その認証情報に基づいて画像形成装置１０００を認証し、認証できた場合のみ、ポリシーとしてＤＳＰ２０００ｂを通信部４１２３によって送信する。

【０２３８】

次に、タイマーによってポリシーを取得する第五のポリシー設定方法について図３７で説明する。

【０２３９】

図３７は、タイマーによってポリシーを取得する第六のポリシー設定方法を示す図である。図３７中、図３３と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０２４０】

図３７において、画像形成装置１０００は、タイマー管理による処理時間が経過すると（ステップＳ５１）、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー配布サーバ４０００にポリシー取得要求を送信し、ポリシー配布サーバ４０００からＳＯＡＰサーバ機能４０２１によって受信結果としてポリシー（管理コンソール４００１から受信したＤＳＰ２０００）を送信する（ステップＳ５２）。

【０２４１】

この第三のポリシー設定方法において、ポリシー配布サーバ４０００はＳＯＡＰクライアント機能４０２１とＳＯＡＰサーバ機能４０２４とを有するようにし、また、画像形成装置１０００はＳＯＡＰサーバ機能２２とＳＯＡＰクライアント機能４０２３とを有するようにして、画像形成装置１０００がポリシー取得要求を行った後にポリシーを配布するように構成しても良い。

【０２４２】

図３７に示す第三のポリシー設定方法を実現する機能構成について図３８で説明する。図３８は、第六のポリシー設定方法を実現するための機能構成の例を示す図である。図３８中、図３６と同様の処理部には同一の符号を付し、その説明を省略する。また、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２－２を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２４３】

図３６に示す動作要件選択部１０１２との違いは、動作要件選択部１０１２－２が、タイマー部４１０５を更に有することである。

【０２４４】

タイマー部４１０５は、所定時間が経過すると、所定時間が経過したことを通信部４１０３に通知する。この通知に応じて、通信部４１０３は、ポリシー配布サーバ４０００からＳＯＡＰに従ってＤＳＰ２０００ｂを取得し、ポリシー書き換え部４１０４がＤＳＰ２０００ａをＤＳＰ２０００ｂで書き換える。

【０２４５】

次に、オフラインでポリシーを設定する方法について図３９で説明する。図３９は、オフラインでポリシーを設定する第七のポリシー設定方法を示す図である。図３９中、図３１と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０２４６】

図３９において、例えば、図２６に示すようなハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、光ディスク５４の記憶媒体５０にＤＳＰ２０００を格納し、その記憶媒体５０を画像形成装置１０００に設定してＤＳＰ２０００を画像形成装置１０００の所定記憶領域に格納することによって、オフラインでポリシーを設定する（ステップＳ７１）。

【０２４７】

その後、画像形成装置１０００は、所定格納領域にポリシーとして格納されたＤＳＰ２０００に従って動作する（ステップＳ７２）。

【０２４８】
図３９に示す第四のポリシー設定方法を実現する機能構成について説明する。図４０は、第七のポリシー設定方法を実現するための機能構成の例を示す図である。図４０中、図３６と同様の処理部には同一の符号を付し、その説明を省略する。図４０における説明において、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２－３を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２４９】
動作要件選択部１０１２－３は、記憶媒体５０から記憶媒体５０に格納されているＤＳＰ２０００を読み取るためのインターフェース４１０６を有するが、通信部４１０３を含めない。

【０２５０】
ポリシー書き換え部４１０４は、インターフェース４１０６によって読み込まれたＤＳＰ２０００を、動作要件選択部１０１２０３が現在保持しているＤＳＰ２０００ａと書き換える。このようにして、オフラインの場合に、ポリシーが設定される。また、例えば、ＤＳＰ２０００が格納された記憶媒体５０によってオフラインでポリシーを設定する場合には、改ざん検知コードなどを追加することによって、ポリシーの信頼性を向上させることができる。

【０２５１】
次に、ポリシーをオフラインで設定し、オンラインで選択する方法について図４１で説明する。図４１は、ポリシーをオフラインで設定し、オンラインで選択する第八のポリシー設定方法を示す。図４１中、図３１と同様の部分には同一の符号を付し、その説明を省略する。また、画像形成装置１０００又は１０００－２を画像形成装置１０００として説明する。

【０２５２】
図４１において、管理者コンソール４００１からポリシー配布サーバ４０００へネットワーク５を介して、例えば、ポリシーとしてＤＳＰ２０００が設定される（ステップＳ８１）。

【０２５３】
また、オフラインでＤＳＰ２０００が格納された記憶媒体５０（図２６に示すようなハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、光ディスク５４）が、画像形成装置１０００のセキュリティポリシーのデータベースに設定される（ステップＳ８２）。

【０２５４】
その後、管理コンソール４００１から、ネットワーク５を介して、ポリシー配布サーバ４０００にポリシーの選択が指定される（ステップＳ８３）。ここで、ポリシーの選択とは、ポリシーの識別情報によってポリシーの１つが選択される。

【０２５５】
ポリシー配布サーバ４０００は、管理コンソール４００１からのポリシー選択に応じて、ＳＯＡＰクライアント機能４０２１を利用して、画像形成装置１０００へポリシー選択を通知する（ステップＳ８４）。画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２を利用して、ポリシー選択通知を受信し、ポリシー配布サーバ４０００に対して受信結果を返す。つまり、執行すべきポリシーの識別情報が画像形成装置１０００に通知される。

【０２５６】
画像形成装置１０００は、ポリシー選択に従って、識別情報で指定されるポリシーを選択し、その選択したポリシーに従って動作する（ステップＳ８５）。

【０２５７】
このような第五のポリシー設定方法を実現する機能構成について図４２で説明する。図４２は、第八のポリシー設定方法を実現するための機能構成の例を示す図である。図４２中、図３６及び図４０と同様の処理部には同一の符号を付し、その説明を省略する。図４

２における説明において、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２－４を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２５８】

動作要件選択部１０１２－４は、通信部４１０３を有すると共に、記憶媒体５０から記憶媒体５０に格納されているＤＳＰ２０００を読み取るための記憶媒体５０に対応したインターフェース４１０６を有する。

【０２５９】

通信部４１０３は、ＳＯＡＰに従ってポリシー配布サーバ４０００－２から受信したポリシー選択をポリシー書き換え部４０１２－２に通知する。

【０２６０】

ポリシー書き換え部４０１２－２は、例えば、オフラインのポリシー設定によって、インターフェース４１０６によって記憶媒体５０に格納されたＤＳＰ２０００を読み込んで、ドキュメントセキュリティポリシーＤＢ９２に格納する。ポリシー書き換え部４０１２－２は、通信部４１０３から通知されたポリシー選択に基づいて、執行すべきポリシーで置き換える。つまり、以前の執行すべきポリシーがＤＳＰ２０００ａであって、識別情報によってＤＳＰ２０００が指定された場合、執行すべきポリシーとしてＤＳＰ２０００ａをＤＳＰ２０００で書き換える。

【０２６１】

また、ポリシー配布サーバ４０００－２が、ＤＳＰ２０００ｂを記憶媒体５０に書き込むためのインターフェース４１２６を有する構成とすることによって、オフラインでポリシーを設定するために、ポリシー管理部４１２４がポリシー配布サーバ４０００－２のＤＳＰ２０００ｂを配布するポリシー（ＤＳＰ２０００）として記憶媒体５０に書き込むようにしても良い。この場合の記憶媒体５０は、図２６に示すようなハードディスク５１、光磁気ディスク５２、フレキシブルディスク５３、又は、光ディスク５４等である。

【０２６２】

ポリシー配布サーバ４０００－２において、通信部４１２３は、ＳＯＡＰに従って、ポリシー選択を画像形成装置１０００へ送信する。

【０２６３】

次に、ドキュメント属性とユーザ属性とに基づくポリシーの解釈を外部サーバに問い合わせる機能構成について図４３及び４４で説明する。

【０２６４】

図４３は、外部サーバがポリシーを解釈する機能構成の例を示す図である。図４３中、図３６と同様の処理部には同一の符号を付し、その説明を省略する。図４３における説明において、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２－３を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２６５】

画像形成装置１０００側において、動作要件選択部１０１２－５は、通信部４１０３－２と、選択要件件勝負４１０２と、システム属性９１ａのみを有する。

【０２６６】

通信部４１０３－２は、ポリシー解釈サーバ４２００とＳＯＡＰに従って通信を制御する処理部である。通信部４１０３－２は、ドキュメント属性取得部１０１１から通知されたドキュメント属性と、ユーザ属性取得部１０２１から通知されたユーザ属性とを、ＳＯＡＰに従ってポリシー解釈サーバ４２００に送信する。また、通信部４１０３－２は、ポリシー解釈サーバ４２００からドキュメント属性とユーザ属性とに応じたルールを受信すると、選択要件検査部４１０２に通知する。ルールには、動作に対して許可する場合、満たさなければならない動作要件が示される。

【０２６７】

選択要件検証部４１０２は、システム属性９１ａを参照しつつ、動作要件を満たすこと

ができるか否かを判断し、その判断結果を動作制御部１０１３に通知する。

【０２６８】

外部サーバとしてのポリシー解釈サーバ４２００は、サーバコンピュータであって、通信部４２１３と、ポリシー解釈部４２２４と、ＤＳＰ２０００ｂとを有する。

【０２６９】

通信部４２１３は、ＳＯＡＰに従って、画像形成装置１０００との通信を制御する処理部であって、画像形成装置１０００から受信したドキュメント属性とユーザ属性とをポリシー解釈部４２２４に通知し、ポリシー解釈部４２２４から通知されたドキュメント属性とユーザ属性とに対応するルールを画像形成装置１０００へ送信する。ルールには動作が許可される場合の動作要件が含まれる。

【０２７０】

ポリシー解釈部４２２４は、通信部４２１３から取得したドキュメント属性とユーザ属性とに基づいて、ＤＳＰ２０００ｂを参照することによって、動作が許可される場合の動作要件を含むルールを取得する。そのルールを通信部４２１３へ通知する。

【０２７１】

このような機能構成によって、画像形成装置１０００がポリシーを保持していなくても、画像形成装置１０００での動作に対してセキュリティポリシーを執行することができる。

【０２７２】

次に、外部サーバが、ポリシーを解釈し、更に選択要件を検証する機能構成について図４４で説明する。

【０２７３】

図４４は、外部サーバがポリシーを解釈し、選択要件を検証する機能構成の例を示す図である。図４４中、図４３と同様の処理部には同一の符号を付し、その説明を省略する。図４３における説明において、画像形成装置１０００と画像形成装置１０００－２とは、同様の動作要件選択部１０１２－３を有するため、画像形成装置１０００で説明する。また、点線の部分１００２は、省略可能であることを示す。

【０２７４】

画像形成装置１０００側において、動作要件選択部１０１２－６は、通信部４１０３－３のみを有する。

【０２７５】

通信部４１０３－３は、ポリシー解釈サーバ４２００とＳＯＡＰに従って通信を制御する処理部である。通信部４１０３－３は、ドキュメント属性取得部１０１１から通知されたドキュメント属性と、ユーザ属性取得部１０２１から通知されたユーザ属性とを、ＳＯＡＰに従ってポリシー解釈サーバ４２００－２に送信する。また、通信部４１０３－２は、ポリシー解釈サーバ４２００から動作に対する許可又は不許可と、許可する場合には動作要件とを受信し、動作制御部１０１３へ通知する。

【０２７６】

外部サーバとしての動作要件選択サーバ４２００－２は、図４３に示される構成に加えて、更に、選択要件検査部４２２６と、システム属性９１ｂとを有する。

【０２７７】

ポリシー解釈部４２２４は、通信部４２１３から取得したドキュメント属性とユーザ属性とに基づいて、ＤＳＰ２０００ｂを参照することによって、動作が許可される場合の動作要件を含むルールを取得して、選択要件検証部４２２６へ通知する。

【０２７８】

選択要件検証部４２２６は、システム属性９１ｂを参照することによって、画像形成装置１０００が動作要件を満たすことができるか否かを判断し、その判断結果を通信部４２１３によって画像形成装置１０００へ送信する。動作要件を画像形成装置１０００が満たすことができないと判断した場合、判断結果は不許可を示す。一方、動作要件を画像形成装置１０００が満たすと判断した場合、判断結果は許可を示すと共に、動作要件を指定す

る。

【０２７９】

次に、画像形成装置１０００の選択要件検証部４１０２によって参照される、画像形成装置１０００内に備えられたシステム属性９１ａについて図４５で説明する。図４５は、画像形成装置内に備えられてシステム属性の例を示す図である。

【０２８０】

図４５において、システム属性９１ａは、通常、ユーザの選択によって実行可能な動作条件の項目を管理するテーブルであって、動作条件、サポートの可否を示すサポート等の項目を有する。動作条件として、ログの記録、イメージログの記録、機密ラベルの印字、操作者ラベルの印字、識別バーコードの印字、識別パターンの印字等が示される。

【０２８１】

通常、動作条件は、動作する際の選択可能な機能として画像形成装置１０００に備えられている。このような動作条件が、ポリシーによって動作を許可する場合の要件として指定される場合、動作要件となる。

【０２８２】

図４６は、外部サーバに備えられたシステム属性の例を示す図である。図４６において、システム属性９１ｂは、動作条件毎に、複数の画像形成装置におけるサポート可否を、画像形成装置の識別情報（装置０１、装置０２、装置０３、装置０４、．．．）と対応付けて管理するテーブルである。動作条件として、ログの記録、イメージログの記録、機密ラベルの印字、操作者ラベルの印字、識別バーコードの印字、識別パターンの印字等が示される。

【０２８３】

通常、動作条件は、動作する際の選択可能な機能である。このような動作条件が、ポリシーによって動作を許可する場合の要件として指定される場合、動作要件となる。

【０２８４】

次に、画像形成装置１０００又は１０００－２とポリシー配布サーバ４０００とで行われるポリシーを設定するためのＳＯＡＰの例について図４７から図５６で説明する。図４７から図５６の説明において、読み取り装置としての画像形成装置１０００と複写装置としての画像形成装置１０００－２とに何ら差異はないため、画像形成装置１０００で説明する。

【０２８５】

先ず、図３１に示されるように、ポリシー配布サーバ４０００が、ＳＯＡＰクライアント機能４０２１を利用して、画像形成装置１０００にポリシー配布を行う場合のＳＯＡＰについて図４７で説明する。図４７は、ＳＯＡＰに従って送信されるポリシー配布を示すＸＭＬデータの例を示す図である。

【０２８６】

図４７において、ＸＭＬデータ８００は、ポリシーを配布するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８００において、<nsl:policyDistribution>を示す記述８０１から</nsl:policyDistribution>を示す記述８０２までに、配布されるポリシーに関する情報と、ポリシー自身が示される。

【０２８７】

記述８０１において、「policyDistribution」により、このＸＭＬデータ８００がポリシーを配布することを示している。

【０２８８】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８０３は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。そして、<policy xsi:type="xsd:string">から</policy>の記述８０４でポリシーが記述される。例えば、識別情報「RDSP2023」で識別されるＤＳＰ２０００（図１４から図２２参照）そのものが記述される。

【０２８９】

そして、このようなポリシー配布を示すＸＭＬデータ８００を受信した画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２を利用して、図４８に示されるような受信結果をポリシー配布サーバ４０００へ送信する。図４８は、ＳＯＡＰに従って送信されるポリシー配布に対する受信結果を示すＸＭＬデータの例を示す図である。

【０２９０】

図４８において、ＸＭＬデータ８１０は、ポリシー配布に対する受信結果を示すＸＭＬによる記述である。ＸＭＬデータ８１０において、<nsl:policyDistributionResponse>を示す記述８１１から</nsl:policyDistributionResponse>を示す記述８１２までに、ポリシー配布に対する受信結果に関する情報が示される。

【０２９１】

記述８１２において、「policyDistributionResponse」によりこのＸＭＬデータ８１０がポリシー配布に対する応答であることを示している。

【０２９２】

<result xsi:type="xsd:boolean">true</result>を示す記述８１３は、ポリシー配布を正常に受信したか否かを示す。この場合、「true」が示されるため、正常に受信したことを示している。

【０２９３】

図３２に示されるように、ポリシー配布サーバ４０００が、ＳＯＡＰクライアント機能４０２１を利用して、画像形成装置１０００にポリシー配布通知を行う場合のＳＯＡＰについて図４９で説明する。図４９は、ＳＯＡＰに従って送信されるポリシー配布通知を示すＸＭＬデータの例を示す図である。

【０２９４】

図４９において、ＸＭＬデータ８２０は、ポリシー配布を通知するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８２０において、<nsl:policyDistributionReport>を示す記述８２１から</nsl:policyDistributionReport>を示す記述８２２までに、ポリシー配布通知に関する情報が示される。

【０２９５】

記述８２１において、「policyDistributionReport」により、このＸＭＬデータ８２０がポリシー配布を通知することを示している。

【０２９６】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８２３は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。

【０２９７】

そして、このようなポリシー配布通知を示すＸＭＬデータ８２０を受信した画像形成装置１０００は、ＳＯＡＰサーバ機能４０２２を利用して受信結果を送信した後、ＳＯＡＰクライアント機能４０２３を利用して、図５０に示されるようなポリシー取得要求をポリシー配布サーバ４０００へ送信する。図５０は、ＳＯＡＰに従って送信されるポリシー取得要求を示すＸＭＬデータの例を示す図である。

【０２９８】

図５０において、ＸＭＬデータ８３０は、ポリシーを配布するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８３０において、<nsl:policyRequest>を示す記述８３１から</nsl:policyRequest>を示す記述８３２までに、ポリシー取得要求に関する情報が示される。

【０２９９】

記述８３１において、「policyRequest」により、このＸＭＬデータ８３０がポリシーの取得を要求していることを示している。

【０３００】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８３３は、図４９に示されるポリシー配布通知を示すＸＭＬデータ８２０で通知されたポリシーを識別するための識別情報「RDSP2023」が設定されている。

【０３０１】
このポリシー取得要求を示すＸＭＬデータ８３０は、ポリシー配布通知を受信後、又は、処理のタイミングでポリシー配布サーバ４０００に送信される。
【０３０２】
そして、このようなポリシー取得要求を示すＸＭＬデータ８３０を受信したポリシー配布サーバ４０００は、ＳＯＡＰサーバ機能４０２４を利用して、図５１に示されるような受信結果を画像形成装置１０００へ送信する。図５１は、ＳＯＡＰに従って送信されるポリシー取得要に求対する受信結果を示すＸＭＬデータの例を示す図である。
【０３０３】
図５１において、ＸＭＬデータ８４０は、ポリシー取得要求に対する受信結果を示すＸＭＬによる記述である。ＸＭＬデータ８４０において、<nsl:policyDistribution>を示す記述８４１から</nsl:policyDistribution>を示す記述８４２までに、配布されるポリシーに関する情報と、ポリシー自身が示される。
【０３０４】
記述８４１において、「policyDistribution」により、このＸＭＬデータ８４０がポリシーを配布することを示している。
【０３０５】
<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８４３は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。そして、<policy xsi:type="xsd:string">から</policy>の記述８４４でポリシーが記述される。例えば、識別情報「RDSP2023」で識別されるＤＳＰ２０００（図１４から図２２参照）そのものが記述される。
【０３０６】
図５２に示されるように、画像形成装置１０００が、ＳＯＡＰクライアント機能４０２３を利用して、ポリシー配布サーバ４０００にポリシー配布要求を行う場合のＳＯＡＰについて図５２で説明する。図５２は、ＳＯＡＰに従って送信されるポリシー配布要求を示すＸＭＬデータの例を示す図である。
【０３０７】
図５２において、ＸＭＬデータ８５０は、ポリシー配布を要求するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８５０において、<nsl:policyDistributionRequest>を示す記述８５１から</nsl:policyDistributionRequest>を示す記述８５２までに、ポリシー配布要求に関する情報が示される。
【０３０８】
記述８５１において、「policyDistributionRequest」により、このＸＭＬデータ８５０がポリシー配布を通知することを示している。
【０３０９】
<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８５３は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。
【０３１０】
そして、このようなポリシー配布要求を示すＸＭＬデータ８５０を受信したポリシー配布サーバ４０００は、受信後直に、或いは、所定のタイミングで図４７に示すＸＭＬデータ８００によってポリシー配布を行う。
【０３１１】
図４１に示されるように、ポリシー配布サーバ４０００が、ＳＯＡＰクライアント機能４０２１を利用して、画像形成装置１０００へポリシー選択通知を行う場合のＳＯＡＰについて図５３で説明する。図５３は、ＳＯＡＰに従って送信されるポリシー選択通知を示すＸＭＬデータの例を示す図である。
【０３１２】
図５３において、ＸＭＬデータ８６０は、ポリシー選択を通知するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８６０において、<nsl:policyChangeRequest

>を示す記述８６１から</nsl:policyChangeRequest>を示す記述８６２までに、選択すべきポリシーに関する情報が示される。

【０３１３】

記述８６１において、「policyChangeRequest」により、このＸＭＬデータ８６０がポリシー選択の通知であることを示している。

【０３１４】

<policyId xsi:type="xsd:string">RDSP2023</policyId>を示す記述８６３は、ポリシーを識別するための識別情報「RDSP2023」が設定されている。画像形成装置１０００は、識別情報「RDSP2023」で識別されるポリシーを執行用のポリシーとして設定する。

【０３１５】

次に、図４３又は図４４において、画像形成装置１０００がポリシーの解釈を行う外部サーバに動作要件取得要求を行う場合のＳＯＡＰについて図５４及び図５５で説明する。図５４及び図５５は、ＳＯＡＰに従って送信される動作要件取得要求を示すＸＭＬデータの例を示す図である。図５４及び図５５によって、一つのＸＭＬデータ８７０が示される。

【０３１６】

ＸＭＬデータ８７０において、図５４の<nsl:isAllowed>を示す記述８７１から図５５の</nsl:isAllowed>を示す記述８７２までに、ユーザ属性、ドキュメント属性、動作情報とが示される。

【０３１７】

<userTicketInfo>を示す記述８７３から</userTicketInfo>を示す記述８７４によって、ユーザ属性が必要な場合のユーザチケットが指定される。例えば、図４３において、外部サーバとしてのポリシー解釈サーバ４２００が、ポリシーを解釈するために、ユーザ属性が必要であると判断した場合、指定されるユーザチケットを用いてユーザ属性を取得する。

【０３１８】

<docInfo xsi:type="nsl:DocInfo">から</docInfo>で示される記述８８１は、ドキュメント属性に関する情報を示す。記述８８１において、<catgory xsi:type="xsd:string">Technical_doc</category>を示す記述８８２は、ドキュメントのカテゴリーが「Technical_doc（技術関連文書）」であることを示し、<level xsi:type="xsd:string">High</level>を示す記述８８３は、ドキュメントのレベルが「High（高レベル）」であることを示し、<zone xsi:type="xsd:string">99.99.99.99</zone>を示す記述８８４は、ゾーンが「99.99.99.99」であることを示している。

【０３１９】

また、<accessInfo>から</accessinfo>を示す記述８８５は、動作情報を示す。記述８８５において、<operation xsi:type="xsd:string">COPY</operation>を示す記述８８６は、動作がコピーであることを示している。

【０３２０】

図４３に示す外部サーバとしてのポリシー解釈サーバ４２００は、このようなＸＭＬデータ８７０を受信すると、図５６に示すようなポリシー解釈部４２２４によるポリシー解釈結果を画像形成装置１０００へ送信する。図５６は、ＳＯＡＰに従って送信されるポリシー解釈結果を示すＸＭＬデータの例を示す図である。

【０３２１】

図５６において、ＸＭＬデータ８９０は、ポリシー解釈結果を通知するためのＳＯＡＰに従ったＸＭＬによる記述である。ＸＭＬデータ８９０において、<nsl:isAllowedResponse>を示す記述８９１から</nsl:isAllowedResponse>を示す記述８９２までに、ポリシー解釈結果に関する情報が示される。

【０３２２】

記述８９１において、「isAllowedResponse」により、このＸＭＬデータ８９０がポリシー解釈結果の通知を示している。

【０３２３】
<allowed xsi:type="xsd:boolean">true</allowed>を示す記述８９５は、動作が許可されたことを示す。
【０３２４】
また、<requirements>から</requirements>までの記述８９６は、動作を許可するための動作要件が示される。記述８９６において、<item>から</item>までの記述８９７は、動作要件を示す。<requirement xsi:type="xsd:string">audit</requirement>を示す記述によって、動作要件として監査証跡の記録（「audit」）が指定される。
【０３２５】
次に、動作制御部１０１３の機能構成について図５７及び図５８で説明する。先ず、図２８に示す読み取り装置としての画像形成装置１０００の動作制御部１０１３の機能構成について説明する。図５７は、読み取り装置としての画像形成装置における動作制御部の機能構成の例を示す図である。
【０３２６】
図５７において、読み取り装置としての画像形成装置１０００において、動作制御部１０１３は、データ処理部７４を制御するデータ処理制御部７４ａと、データ送信部７５を制御するデータ送信制御部７５ａとを有する。
【０３２７】
読み取り装置としての画像形成装置１０００において、データ処理制御部７４ａは、例えば、動作要件選択部１０１２から通知された動作要件に従って、読み取り処理を停止し、必要に応じて読み取ったデータを全て消去する、読み取ったデータの一部を黒くする、白くする、又はページを削除する等によって消去する、カラー情報を消去する、情報量を低減する、「丸秘」スタンプを印字することよって機密ラベルを追加する、また、バーコード、数字、文字、パターン、セキュリティ属性を印字することによって識別情報を追加する、などを実行するようにデータ処理部７４を制御する。
【０３２８】
読み取り装置としての画像形成装置１０００において、データ送信制御部７５ａは、例えば、動作要件選択部１０１２から通知された動作要件に従って、送信を停止する、動作要件で指定された送信先だけに送信する、動作要件で指定された送信先にも送信する、などを実行するようにデータ送信部７５を制御する。
【０３２９】
図５８は、複写装置としての画像形成装置における動作制御部の機能構成の例を示す図である。
【０３３０】
図５８において、複写装置としての画像形成装置１０００－２において、動作制御部１０１３は、データ処理部７４を制御するデータ処理制御部７４ａと、印刷部７６を制御する印刷制御部７６ａとを有する。
【０３３１】
複写装置としての画像形成装置１０００－２において、データ処理制御部７４ａは、図５７の読み取り装置としての画像形成装置１０００におけるデータ処理制御部７４ａと同様であって、例えば、動作要件選択部１０１２から通知された動作要件に従って、読み取り処理を停止し、必要に応じて読み取ったデータを全て消去する、読み取ったデータの一部を黒くする、白くする、又はページを削除する等によって消去する、カラー情報を消去する、情報量を低減する、「丸秘」スタンプを印字することよって機密ラベルを追加する、また、バーコード、数字、文字、パターン、セキュリティ属性を印字することによって識別情報を追加する、などを実行するようにデータ処理部７４を制御する。
【０３３２】
複写装置としての画像形成装置１０００－２において、印刷制御部７６ａは、例えば、印刷を停止する、動作要件で指定されたトレイの用紙に印刷する、などを実行するように印刷制御部７６ａを制御する。

【０３３３】
上記実施例において、読み取り装置としての画像形成装置１０００と、複写装置としての画像形成装置１０００－２について例示したが、プリンタ、ＦＡＸ、コピー等の複数の異なる画像形成機能の少なくとも１つを有する装置又はこのような複数の異なる画像形成機能を有する装置であっても良い。
【０３３４】
本発明によれば、ドキュメントに関する企業内のセキュリティポリシーを外部から設定できるため、企業内を一貫したセキュリティポリシーによってドキュメントの取り扱いを制御することができる。また、ドキュメントが紙原稿であっても電子データ（ドキュメントデータ）であっても、セキュリティポリシーに従った制御を実行することができる。
【図面の簡単な説明】
【０３３５】
【図１】セキュリティポリシーの例を示す図である。
【図２】ドキュメントラベル用語ファイルのリストの例を示す図である。
【図３】ポリシー用語ファイルの例を示す図である。
【図４】ポリシー用語ファイルの例を示す図である。
【図５】ポリシー用語ファイルの例を示す図である。
【図６】ポリシー用語ファイルの例を示す図である。
【図７】ポリシー用語ファイルの例を示す図である。
【図８】ポリシー用語ファイルの例を示す図である。
【図９】ポリシー用語ファイルの例を示す図である。
【図１０】ポリシー用語ファイルの例を示す図である。
【図１１】ポリシー用語ファイルの例を示す図である。
【図１２】ポリシー用語ファイルの例を示す図である。
【図１３】ポリシー用語ファイルの例を示す図である。
【図１４】ポリシーファイルの例を示す図である。
【図１５】ポリシーファイルの例を示す図である。
【図１６】ポリシーファイルの例を示す図である。
【図１７】ポリシーファイルの例を示す図である。
【図１８】ポリシーファイルの例を示す図である。
【図１９】ポリシーファイルの例を示す図である。
【図２０】ポリシーファイルの例を示す図である。
【図２１】ポリシーファイルの例を示す図である。
【図２２】ポリシーファイルの例を示す図である。
【図２３】ＤＳＰの識別情報の例を示す図である。
【図２４】ＤＳＰの構造を説明するための記述例を示す図である。
【図２５】ＤＳＰの他の記述例を示す図である
【図２６】ＤＳＰを蓄積し且つ配布する種々の媒体を示す図である。
【図２７】本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。
【図２８】セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。
【図２９】簡略化したＤＳＰの例を示す図である。
【図３０】セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。
【図３１】外部サーバからポリシーが配布される第一のポリシー設定方法を示す図である。
【図３２】外部サーバからポリシーを取得する第二のポリシー設定方法を示す図である。
【図３３】電源投入時にポリシーを取得する第三のポリシー設定方法を示す図である

。
【図３４】電源投入時にポリシーを取得する第四のポリシー設定方法を示す図である。
【図３５】電源投入時にポリシーを取得する第五のポリシー設定方法を示す図である。
【図３６】第一から第五のポリシー設定方法を実現するための機能構成の例を示す図である。
【図３７】タイマーによってポリシーを取得する第六のポリシー設定方法を示す図である。
【図３８】第六のポリシー設定方法を実現するための機能構成の例を示す図である。
【図３９】オフラインでポリシーを設定する第七のポリシー設定方法を示す図である。
【図４０】第七のポリシー設定方法を実現するための機能構成の例を示す図である。
【図４１】ポリシーをオフラインで設定し、オンラインで選択する第八のポリシー設定方法を示す。
【図４２】第八のポリシー設定方法を実現するための機能構成の例を示す図である。
【図４３】外部サーバがポリシーを解釈する機能構成の例を示す図である。
【図４４】外部サーバがポリシーを解釈し、選択要件を検証する機能構成の例を示す図である。
【図４５】画像形成装置内に備えられてシステム属性の例を示す図である。
【図４６】外部サーバに備えられたシステム属性の例を示す図である。
【図４７】ＳＯＡＰに従って送信されるポリシー配布を示すＸＭＬデータの例を示す図である。
【図４８】ＳＯＡＰに従って送信されるポリシー配布に対する受信結果を示すＸＭＬデータの例を示す図である。
【図４９】ＳＯＡＰに従って送信されるポリシー配布通知を示すＸＭＬデータの例を示す図である。
【図５０】ＳＯＡＰに従って送信されるポリシー取得要求を示すＸＭＬデータの例を示す図である。
【図５１】ＳＯＡＰに従って送信されるポリシー取得要求に対する受信結果を示すＸＭＬデータの例を示す図である。
【図５２】ＳＯＡＰに従って送信されるポリシー配布要求を示すＸＭＬデータの例を示す図である。
【図５３】ＳＯＡＰに従って送信されるポリシー選択通知を示すＸＭＬデータの例を示す図である。
【図５４】ＳＯＡＰに従って送信されるポリシー選択通知を示すＸＭＬデータの例を示す図である。
【図５５】ＳＯＡＰに従って送信されるポリシー配布を示すＸＭＬデータの例を示す図である。
【図５６】ＳＯＡＰに従って送信されるポリシー解釈結果を示すＸＭＬデータの例を示す図である。
【図５７】読み取り装置としての画像形成装置における動作制御部の機能構成の例を示す図である。
【図５８】複写装置としての画像形成装置における動作制御部の機能構成の例を示す図である。

【符号の説明】

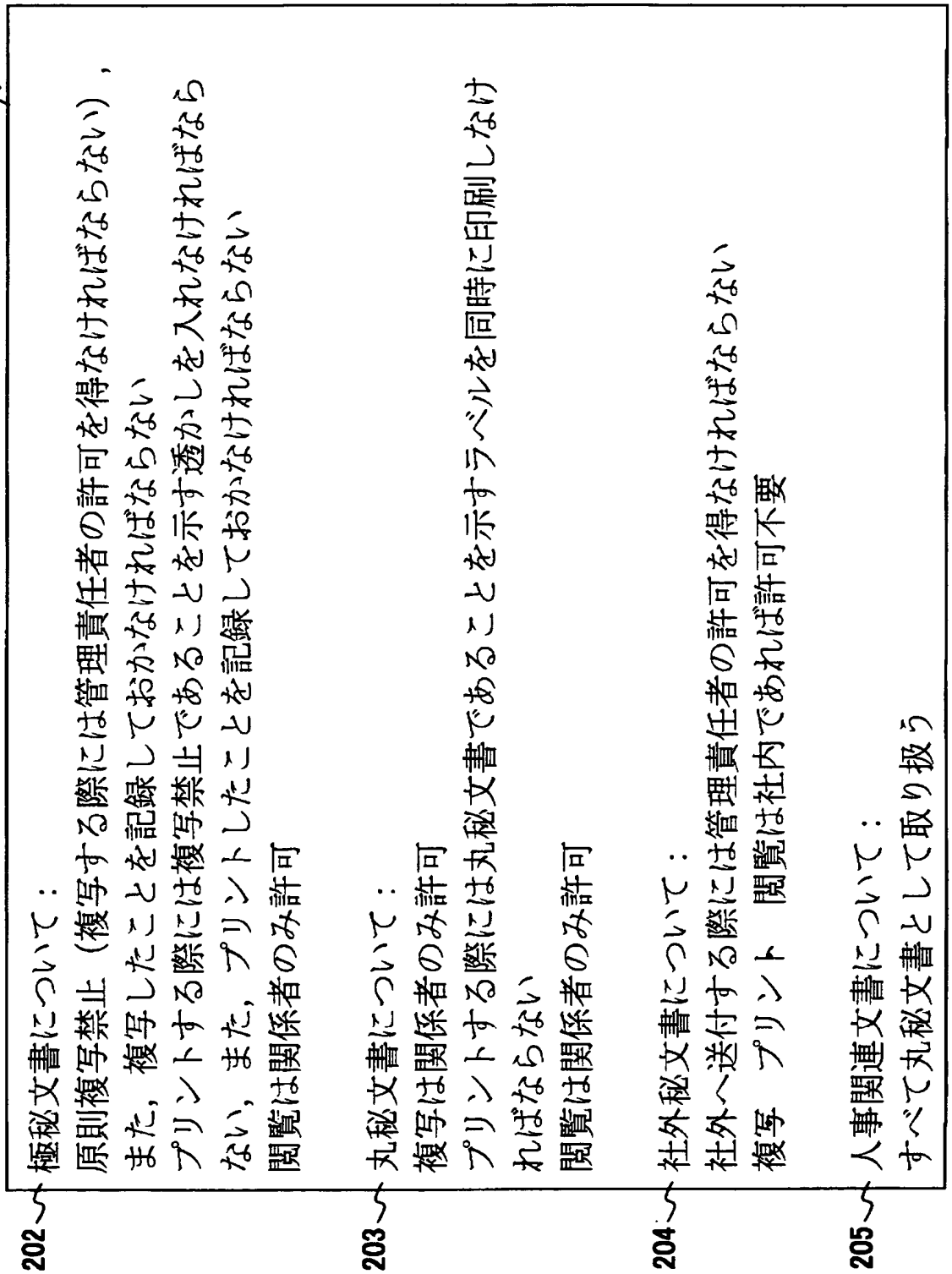
【０３３６】

５１　　ハードディスク
５２　　光磁気ディスク
５３　　フレキシブルディスク

５４	光ディスク
５５	コンピュータ
５６	ネットワーク
７１	読み取り部
７２	読み取り条件取得部
７３	データ送信先取得部
７４	データ処理部
１０００	画像形成装置
１００１	ポリシー実行部
１０１１	ドキュメント属性取得部
１０１２	動作要件選択部
１０１３	動作制御部
１０２１	ユーザ属性取得部
２０００	ＤＳＰ

【書類名】図面
【図１】

ドキュメントに関するセキュリティポリシーの例を示す図



【図２】

ドキュメントラベルファイルの例を示す図

300

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_label_terminology>
<about_this_terminology>
     <serial_number>RDST0001</serial_number>
     <title>
          DOCUMENT-LABEL-TERMINOLOGY
     </title>
     <version>1.00</version>
     <creation_date>2001/12/21 13:37:18</creation_date>
     <creator>Taro Tokyo</creator>
     <description>sample document-label terminology.</description>
</about_this_terminology>
<enumeration>
312 <enum_id>doc_category</enum_id>
313 <enum_name>Document Category</enum_name>
314 <description>文書カテゴリーの種類</description>
     <item>
315          <name>internal_doc</name>
          <description>社内一般文書</description>
     </item>
311  <item>
316          <name>human_resource_doc</name>
          <description>人事関連文書</description>
     </item>
     <item>
317          <name>technical_doc</name>
          <description>技術関連文書</description>
     </item>
</enumeration>
<enumeration>
322 <enum_id>doc_security_level</enum_id>
323 <enum_name>Document Security Level</enum_name>
324 <description>文書のセキュリティレベルの種類</description>
     <item>
325          <name>basic</name>
          <description>社外秘</description>
     </item>
321  <item>
326          <name>medium</name>
          <description>秘</description>
     </item>
     <item>
327          <name>high</name>
          <description>極秘</description>
     </item>
</enumeration>
</document_label_terminology>
```

【図３】

ポリシー用語ファイルの例を示す図

400

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
<about_this_terminology>
      <serial_number>RDST9487</serial_number>
      <title>DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
      <version>1.00</version>
      <creation_date>2001/12/21 13:37:18</creation_date>
      <creator>Taro Tokyo</creator>
      <description>sample policy terminology.</description>
</about_this_terminology>

<!-- システムタイプの列挙 -->
<enumeration>
      <enum_id>system_type</enum_id>
      <enum_name>System Type</enum_name>
      <description>システムタイプの種類</description>
      <item>
            <name>Copier</name>
            <description>複写機</description>
            <operation>copier_operation</operation>
      </item>
      <item>
            <name>Printer</name>
            <description>プリンタ</description>
            <operation>printer_operation</operation>
      </item>
      <item>
            <name>Facsimile</name>
            <description>ファクシミリ</description>
            <operation>fax_operation</operation>
      </item>
      <item>
            <name>Scanner</name>
            <description>スキャナ</description>
            <operation>scanner_operation</operation>
      </item>
      <item>
            <name>Document Repository</name>
            <description>文書リポジトリ</description>
            <operation>repository_operation</operation>
      </item>
      <item>
            <name>E-Meeting</name>
            <description>電子会議システム</description>
            <operation>emeeting_operation</operation>
      </item>
</enumeration>
```

411

【図４】

ポリシー用語ファイルの例を示す図

400

```
<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
      <enum_id>copier_operation</enum_id>
      <enum_name>Copier Operation</enum_name>
      <description>複写機に関わるオペレーション</description>
      <item>
            <name>hardcopy</name>
            <description>紙から紙への複写</description>
            <requirement>hardcopy_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>printer_operation</enum_id>
      <enum_name>Printer Operation</enum_name>
      <description>プリンタに関わるオペレーション</description>
      <item>
            <name>print</name>
            <description>電子文書を紙へ印刷</description>
            <requirement>print_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>fax_operation</enum_id>
      <enum_name>Facsimile Operation</enum_name>
      <description>ファックスに関わるオペレーション</description>
      <item>
            <name>fax_send</name>
            <description>ファックスの送信</description>
            <requirement>fax_send_requirement</requirement>
      </item>
      <item>
            <name>fax_receive</name>
            <description>ファックスの受信</description>
            <requirement>fax_receive_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>scanner_operation</enum_id>
      <enum_name>Scanner Operation</enum_name>
      <description>スキャナに関わるオペレーション</description>
      <item>
            <name>scan</name>
            <description>紙文書をスキャンして電子文書にする</description>
            <requirement>scan_requirement</requirement>
      </item>
</enumeration>
```

421　431　441　451

【図５】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>repository_operation</enum_id>
      <enum_name>Document Repository Operation</enum_name>
      <description>文書リポジトリに関わるオペレーション</description>
      <item>
            <name>store</name>
            <description>保存する</description>
            <requirement>store_requirement</requirement>
      </item>
      <item>
            <name>revise</name>
            <description>改訂・編集する</description>
            <requirement>revise_requirement</requirement>
      </item>
      <item>
            <name>delete</name>
            <description>削除・破棄する</description>
            <requirement>delete_requirement</requirement>
      </item>
      <item>
            <name>read</name>
            <description>参照する</description>
            <requirement>read_requirement</requirement>
      </item>
      <item>
            <name>net_delivery</name>
            <description>
             ネットワークで配布する（送信する）
            </description>
      <requirement>net_delivery_requirement</requirement>
      </item>
      <item>
            <name>disc_delivery</name>
            <description>ディスクで配布する（送付する）</description>
            <requirement>disc_delivery_requirement</requirement>
      </item>
      <item>
            <name>archive</name>
            <description>アーカイブ・バックアップする</description>
            <requirement>archive_requirement</requirement>
      </item>
</enumeration>
<enumeration>
      <enum_id>emeeting_operation</enum_id>
      <enum_name>E-Meeting Operation</enum_name>
      <description>電子会議システムに関わるオペレーション</description>
 <item>
            <name>meeting_use</name>
            <description>会議で利用する</description>
            <requirement>meeting_use_requirement</requirement>
      </item>
</enumeration>
```

461

471

【図６】

ポリシー用語ファイルの例を示す図

400

```
<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証，文書識別，アクセス制御（利用制限）は基本メカニズムとして提供されるため
，要件には含めない -->
<enumeration>
      <enum_id>hardcopy_requirement</enum_id>
      <enum_name>Hardcopy Requirement</enum_name>
      <description>複写に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>print_requirement</enum_id>
      <enum_name>Print Requirement</enum_name>
      <description>印刷に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>private_access</name>
            <description>プリントした本人による紙出力</description>
      </item>
 <item>
            <name>trusted_channel</name>
            <description>
             信頼チャネルの利用（印刷データの暗号化）
            </description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             プリントアウトに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
```

481

491

【図７】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>fax_send_requirement</enum_id>
      <enum_name>Requirement on Sending Fax Message</enum_name>
      <description>ファクス送信に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>destination_restriction</name>
            <description>宛先制限</description>
      </item>
501   <item>
            <name>private_mode</name>
            <description>親展モードでの送信</description>
      </item>
      <item>
            <name>trusted_channel</name>
            <description>
                  信頼チャネルの利用（ファクスデータの暗号化）
            </description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
                  送信ファクスに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
      <item>
            <name>non_repudiation</name>
            <description>否認防止（受取証の取得）</description>
      </item>
</enumeration>
```

【図８】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>fax_receive_requirement</enum_id>
      <enum_name>Requirement on Receiving Fax Message</enum_name>
      <description>ファックス受信に関わる要件</description>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>private_access</name>
            <description>親展ファックスの宛先本人による取り出し</description>
      </item>
      <item>
            <name>trusted_timestamp</name>
            <description>信頼タイムスタンプ</description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             受信ファックスに追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
<enumeration>
      <enum_id>scan_requirement</enum_id>
      <enum_name>Scan Requirement</enum_name>
      <description>スキャンに関わる要件（保存した後については保存要件を適用する）
      </description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>embed_trace_info</name>
            <description>
             スキャン画像に追跡情報埋め込み（透かし，ラベル，バーコード）
            </description>
      </item>
</enumeration>
```

511

521

【図９】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>store_requirement</enum_id>
      <enum_name>Store Requirement</enum_name>
      <description>保存に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>保存データの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>保存データの改ざん保護</description>
      </item>
</enumeration>
```

531

```
<enumeration>
      <enum_id>revise_requirement</enum_id>
      <enum_name>Revise Requirement</enum_name>
      <description>改訂に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>versioning</name>
            <description>バージョン管理</description>
      </item>
</enumeration>
```

541

【図１０】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>delete_requirement</enum_id>
      <enum_name>Delete Requirement</enum_name>
      <description>削除・破棄に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>complete_erase</name>
            <description>完全消去</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>read_requirement</enum_id>
      <enum_name>Read Requirement</enum_name>
      <description>参照に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ参照許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ参照許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ参照許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ参照許可</description>
      </item>
</enumeration>
```

551

561

【図１１】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>net_delivery_requirement</enum_id>
      <enum_name>Delivery via Network Requirement</enum_name>
      <description>ネットワーク配信（送信）に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>trusted_channel</name>
            <description>信頼チャネルの利用（送信データの暗号化）
</description>
      </item>
      <item>
            <name>destination_restriction</name>
            <description>宛先制限（社内のみ配信可能など）</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ配信許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ配信許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ配信許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ配信許可</description>
      </item>
</enumeration>
```

571

【図１２】

ポリシー用語ファイルの例を示す図

400

581

```
<enumeration>
      <enum_id>disc_delivery_requirement</enum_id>
      <enum_name>Delivery via Disc Requirement</enum_name>
      <description>ディスク配布（送付）に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>送付データの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>送付データの改ざん保護</description>
      </item>
      <item>
            <name>edit_restriction</name>
            <description>編集禁止のデータのみ送付許可</description>
      </item>
      <item>
            <name>print_restriction</name>
            <description>印刷禁止のデータのみ送付許可</description>
      </item>
      <item>
            <name>location_restriction</name>
            <description>参照場所限定のデータのみ送付許可</description>
      </item>
      <item>
            <name>user_restriction</name>
            <description>ユーザ限定のデータのみ送付許可</description>
      </item>
</enumeration>
```

【図１３】

ポリシー用語ファイルの例を示す図

400

```
<enumeration>
      <enum_id>archive_requirement</enum_id>
      <enum_name>Archive Requirement</enum_name>
      <description>アーカイブ・バックアップに関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>encryption</name>
            <description>アーカイブデータの暗号化</description>
      </item>
      <item>
            <name>integrity_protection</name>
            <description>アーカイブデータの改ざん保護</description>
      </item>
</enumeration>
<enumeration>
      <enum_id>meeting_use_requirement</enum_id>
      <enum_name>Meeting-use Requirement</enum_name>
      <description>会議での利用に関わる要件</description>
      <item>
            <name>explicit_authorization</name>
            <description>明示的な許可（利用制限）</description>
      </item>
      <item>
            <name>audit</name>
            <description>監査証跡の記録</description>
      </item>
      <item>
            <name>audit_with_image</name>
            <description>監査証跡のイメージ付き記録</description>
      </item>
</enumeration>
</policy_terminology>
```

591

601

【図１４】

ポリシーファイルの例を示す図

2000

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<about_this_policy>
     <serial_number>RDSP2023</serial_number>
     <terminology_applied>RDST9487</terminology_applied>
     <title>DOCUMENT-SECURITY-POLICY</title>
     <version>1.30</version>
     <creation_date>2002/02/18 22:30:24</creation_date>
     <creator>Taro Tokyo</creator>
     <description>sample document security policy.</description>
</about_this_policy>
<policy>                                                    2001
     <acc_rule>                                             2011
          <doc_category>ANY</doc_category>                  2013
          <doc_security_level>basic</doc_security_level>    2013
          <acl>
               <ace>
                    <user_category>ANY</user_category>      2017
                    <user_security_level>ANY</user_security_level>  2017
                    <operation>
                         <name>hardcopy</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>print</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>fax_send</name>
                         <requirement>audit</requirement>
                         <requirement>explicit_authorization</requirement>
                    </operation>
                    <operation>
                         <name>fax_receive</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
                    <operation>
                         <name>scan</name>
                         <allowed/><!-- allowed without any requirement -->
                    </operation>
```

【図１５】

ポリシーファイルの例を示す図

2000

```
                <operation>
                    <name>store</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>revise</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>delete</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>read</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>net_delivery</name>
                    <requirement>audit</requirement>
                    <requirement>explicit_authorization</requirement>
                    <requirement>print_restriction</requirement>
                    <requirement>trusted_channel</requirement>
                </operation>
                <operation>
                    <name>disc_delivery</name>
                    <requirement>audit</requirement>
                    <requirement>explicit_authorization</requirement>
                    <requirement>print_restriction</requirement>
                </operation>
                <operation>
                    <name>archive</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                    <name>meeting_use</name>
                    <allowed/><!-- allowed without any requirement -->
                </operation>
            </ace>
        </acl>
    </acc_rule>
```

2012

【図１６】

ポリシーファイルの例を示す図

2000

```
<acc_rule>                                          2021
2023 { <doc_category>ANY</doc_category>
       <doc_security_level>medium</doc_security_level>
       <acl>
            <ace>
       2027 { <user_category>DOC-CATEGORY</user_category>
              <user_security_level>ANY</user_security_level>
              <operation>
                   <name>hardcopy</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>print</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>fax_send</name>
                   <denied/>
                   <!-- denied even if it is explicitly authorized -->
              </operation>
              <operation>
                   <name>fax_receive</name>
                   <allowed/><!-- allowed without any requirement -->
              </operation>
              <operation>
                   <name>scan</name>
                   <requirement>audit</requirement>
                   <requirement>embed_trace_info</requirement>
              </operation>
              <operation>
                   <name>store</name>
                   <allowed/><!-- allowed without any requirement -->
              </operation>
```

【図１７】

ポリシーファイルの例を示す図

2000

```
        <operation>
            <name>revise</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>delete</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>read</name>
            <requirement>audit</requirement>
            <requirement>print_restriction</requirement>
            <requirement>location_restriction</requirement>
        </operation>
        <operation>
            <name>net_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>print_restriction</requirement>
            <requirement>trusted_channel</requirement>
        </operation>
        <operation>
            <name>disc_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>print_restriction</requirement>
        </operation>
        <operation>
            <name>archive</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
            <name>meeting_use</name>
            <allowed/><!-- allowed without any requirement -->
        </operation>
    </ace>
```

【図１８】

ポリシーファイルの例を示す図

2000

```
<acc>
2028 <user_category>ANY</user_category>
     <user_security_level>ANY</user_security_level>
     <operation>
          <name>hardcopy</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>print</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>fax_send</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>fax_receive</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>scan</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>store</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>revise</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
     <operation>
          <name>delete</name>
          <denied/>
          <!-- denied even if it is explicitly authorized -->
     </operation>
```

【図１９】

ポリシーファイルの例を示す図

2000

```
                <operation>
                    <name>read</name>
                    <requirement>explicit_authorization</requirement>
                    <requirement>audit</requirement>
                    <requirement>print_restriction</requirement>
                    <requirement>location_restriction</requirement>
                </operation>
                <operation>
                    <name>net_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>disc_delivery</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>archive</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>meeting_use</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
            </ace>
        </acl>
    </acc_rule>  2022
    <acc_rule>  2031
2033 <doc_category>ANY</doc_category>
     <doc_security_level>high</doc_security_level>
        <acl>
            <ace>
2037 <user_category>DOC-CATEGORY</user_category>
     <user_security_level>ANY</user_security_level>
                <operation>
                    <name>hardcopy</name>
                    <denied/>
                    <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                    <name>print</name>
                    <requirement>explicit_authorization</requirement>
                    <requirement>audit</requirement>
                    <requirement>private_access</requirement>
                    <requirement>trusted_channel</requirement>
                    <requirement>embed_trace_info</requirement>
                </operation>
```

【図２０】

ポリシーファイルの例を示す図

2000

```
<operation>
     <name>fax_send</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
     <name>fax_receive</name>
     <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
     <name>scan</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
     <name>store</name>
     <requirement>audit</requirement>
     <requirement>encryption</requirement>
     <requirement>integrity_protection</requirement>
</operation>
<operation>
     <name>revise</name>
     <requirement>versioning</requirement>
</operation>
<operation>
     <name>delete</name>
     <requirement>complete_erase</requirement>
</operation>
<operation>
     <name>read</name>
     <requirement>audit</requirement>
     <requirement>print_restriction</requirement>
     <requirement>location_restriction</requirement>
     <requirement>user_restriction</requirement>
</operation>
<operation>
     <name>net_delivery</name>
     <denied/>
     <!-- denied even if it is explicitly authorized -->
</operation>
```

【図２１】

ポリシーファイルの例を示す図

2000

```
        <operation>
            <name>disc_delivery</name>
            <requirement>audit</requirement>
            <requirement>explicit_authorization</requirement>
            <requirement>encryption</requirement>
            <requirement>print_restriction</requirement>
        </operation>
        <operation>
            <name>archive</name>
            <requirement>encryption</requirement>
            <requirement>integrity_protection</requirement>
        </operation>
        <operation>
            <name>meeting_use</name>
            <requirement>explicit_authorization</requirement>
        </operation>
    </ace>
    <ace>
2038{   <user_category>ANY</user_category>
    {   <user_security_level>ANY</user_security_level>
        <operation>
            <name>hardcopy</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>print</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_send</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_receive</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
        <operation>
            <name>scan</name>
            <denied/>
            <!-- denied even if it is explicitly authorized -->
        </operation>
```

【図２２】

ポリシーファイルの例を示す図

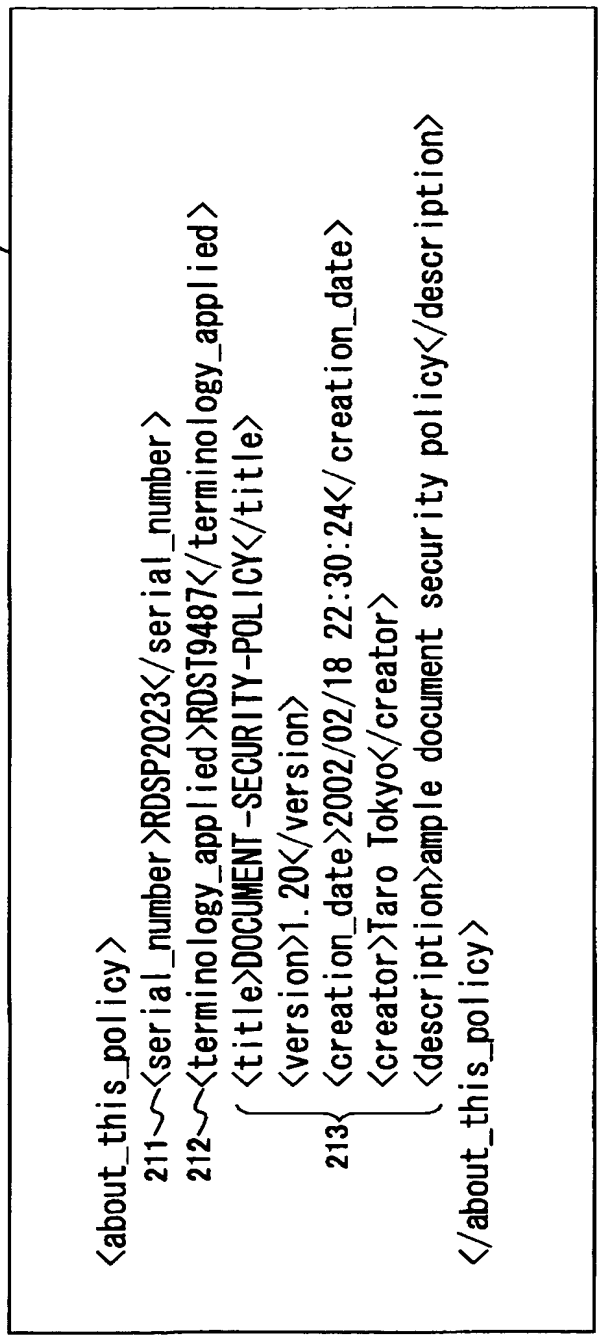
2000

```
                    <operation>
                        <name>store</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                    <operation>
                        <name>revise</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized   >
                    </operation>
                    <operation>
                        <name>delete</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                    <operation>
                        <name>read</name>
                        <requirement>explicit_authorization</requirement>
                        <requirement>audit</requirement>
                        <requirement>print_restriction</requirement>
                        <requirement>location_restriction</requirement>
                        <requirement>user_restriction</requirement>
                    </operation>
                    <operation>
                        <name>net_delivery</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                    <operation>
                        <name>disc_delivery</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                    <operation>
                        <name>archive</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                    <operation>
                        <name>meeting_use</name>
                        <denied/>
                        <!-- denied even if it is explicitly authorized -->
                    </operation>
                </ace>
            </acl>
        </acc_rule>
2002    </policy>
    </document_security_policy>
```

2032

【図２３】

DSPの識別情報を示す図



【図２４】

DSPの構造を説明するための記述例を示す図

220

```
<policy>
221 <acc_rule>
      232 <doc_category>ANY</doc_category>
          <doc_security_level>medium</doc_security_level>
    223 <acl>
          224 <ace>
                225 <user_category>DOC-CATEGORY
                    </user_category>
                226 <user_security_level>ANY
                    </user_security_level>
                227 <operation>
                      228 <name>fax_send</name>
                      229 <denied/><!-- denied even if it
                            is explicitly authorized -->
                    </operation>
                227 <operation>
                      <name>net_delivery</name>
                      230 <requirement>audit
                      </requirement>
                      231 <requirement>
                            explicit_authorization
                      </requirement>
                      ...
                    </operation>
                227 <operation>
                      <name>fax_receive</name>
                      232 <allowed/><!-allowed
                        without requirements -->
                    </operation>
                    ...
              </ace>
              <ace>
                    ...
              </ace>
        </acl>
    </acc_rule>
221 <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>high</doc_security_level>
        <acl>
            ...
        </acl>
    </acc_rule>
</policy>
```

【図２５】

DSPの他の記述例を示す図

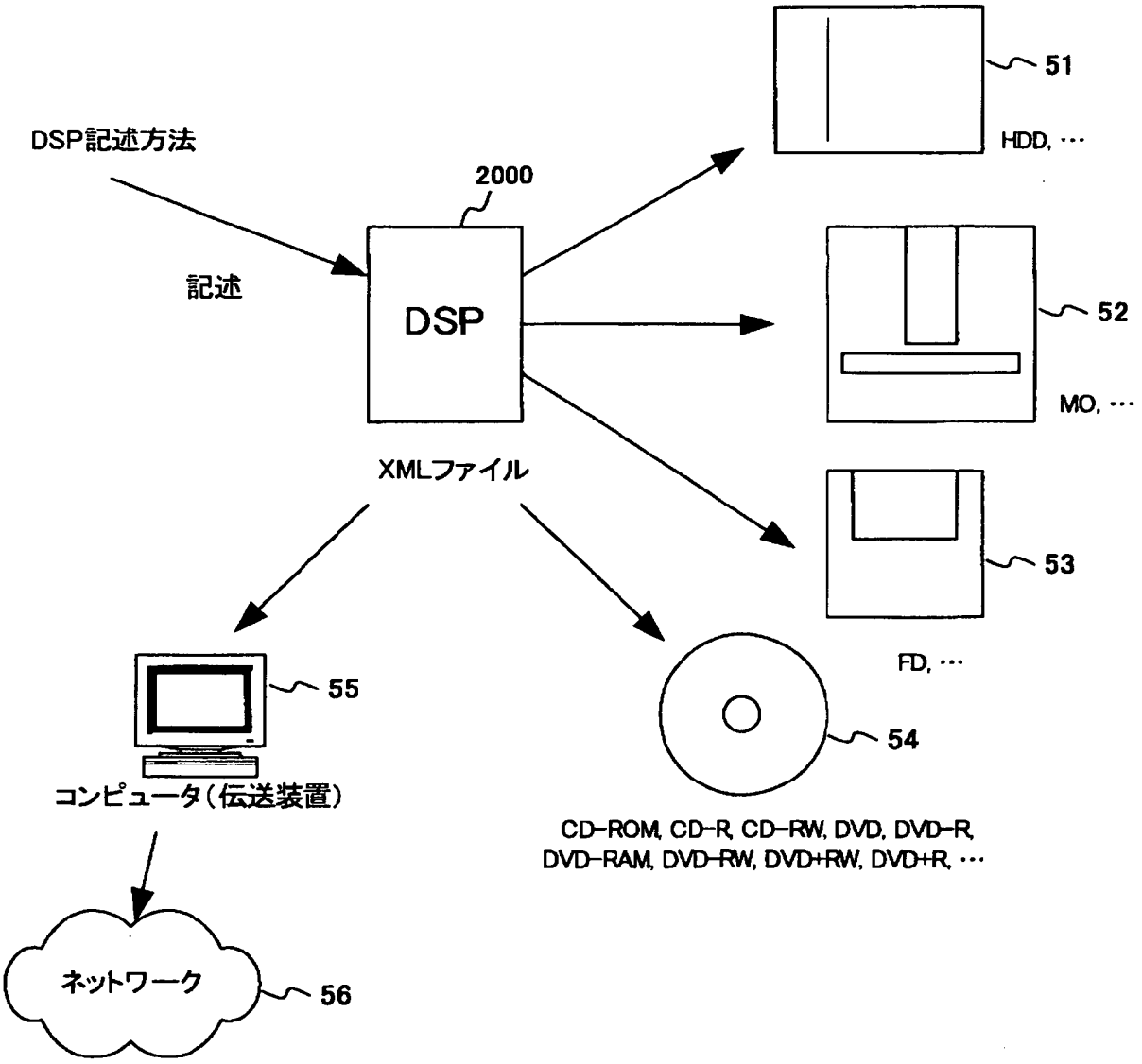
240

```
<policy>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
        <acl>
            <ace>
                <user_category>DOC-CATEGORY</user_category>

<user_security_level>ANY</user_security_level>
241~~<denied_operations>
                <!-- denied even if it is explicitly
                 authorized -->
                    <name>fax_send</name>
                </denied_operations>
                <operation>
                    <name>net_delivery</name>
                    <requirement>audit</requirement>
242~~<requirement>explicit_authorization
                    </requirement>
                                ...
                </operation>
                <operation>
                                ...
                </operation>
243~~<allowed_operations> <!-- allowed without
                                requirements -->
                    <name>fax_receive</name>
                    <name>store</name>
                                ...
                </allowed_operations>
            </ace>
            <ace>
                        ...
            </ace>
                        ...
        </acl>
    </acc_rule>
    <acc_rule>
        <doc_category>ANY</doc_category>
        <doc_security_level>high</doc_security_level>
        <acl>
                    ...
        </acl>
    </acc_rule>
</policy>
```

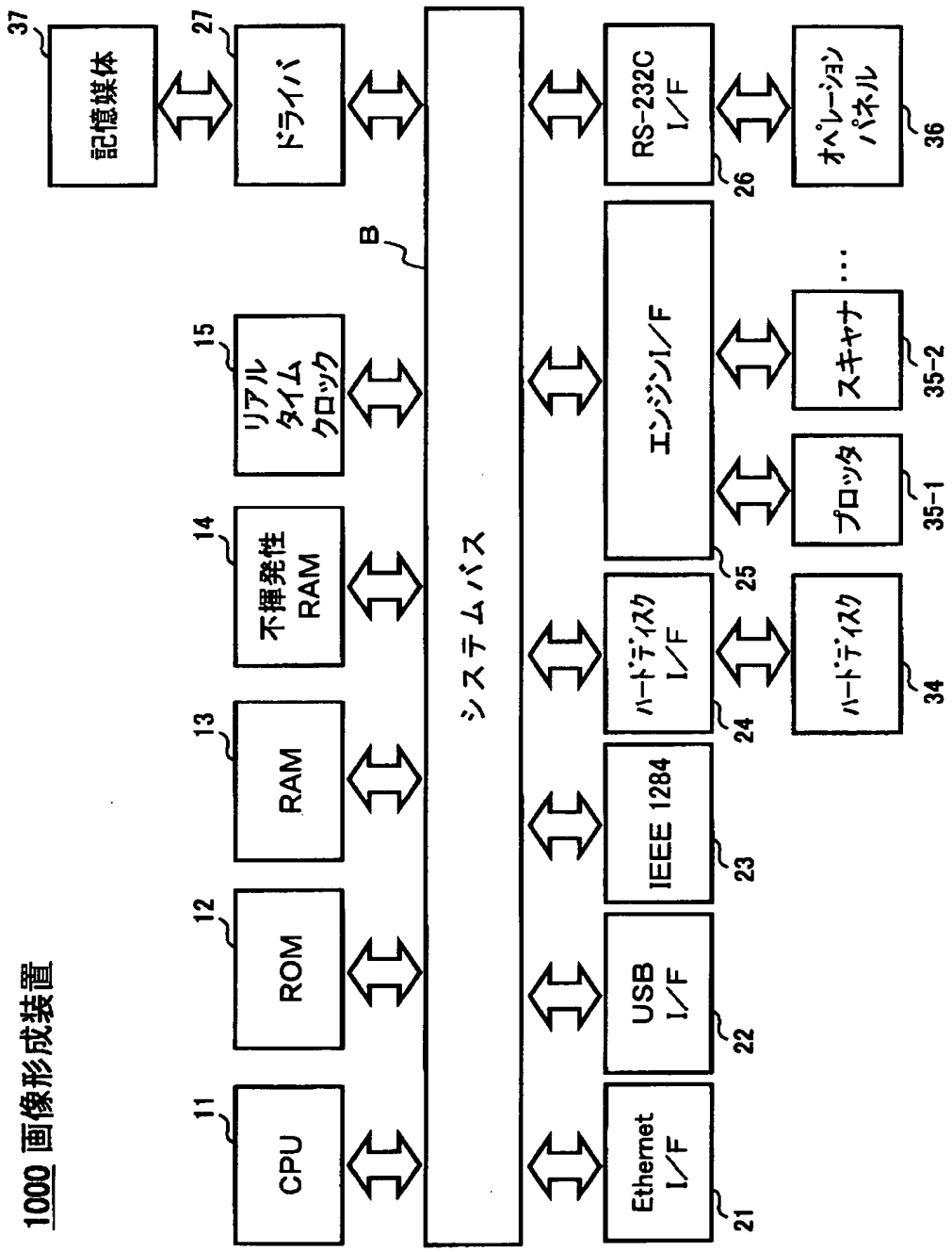
【図２６】

DSPを蓄積し且つ配布する種々の媒体を示す図



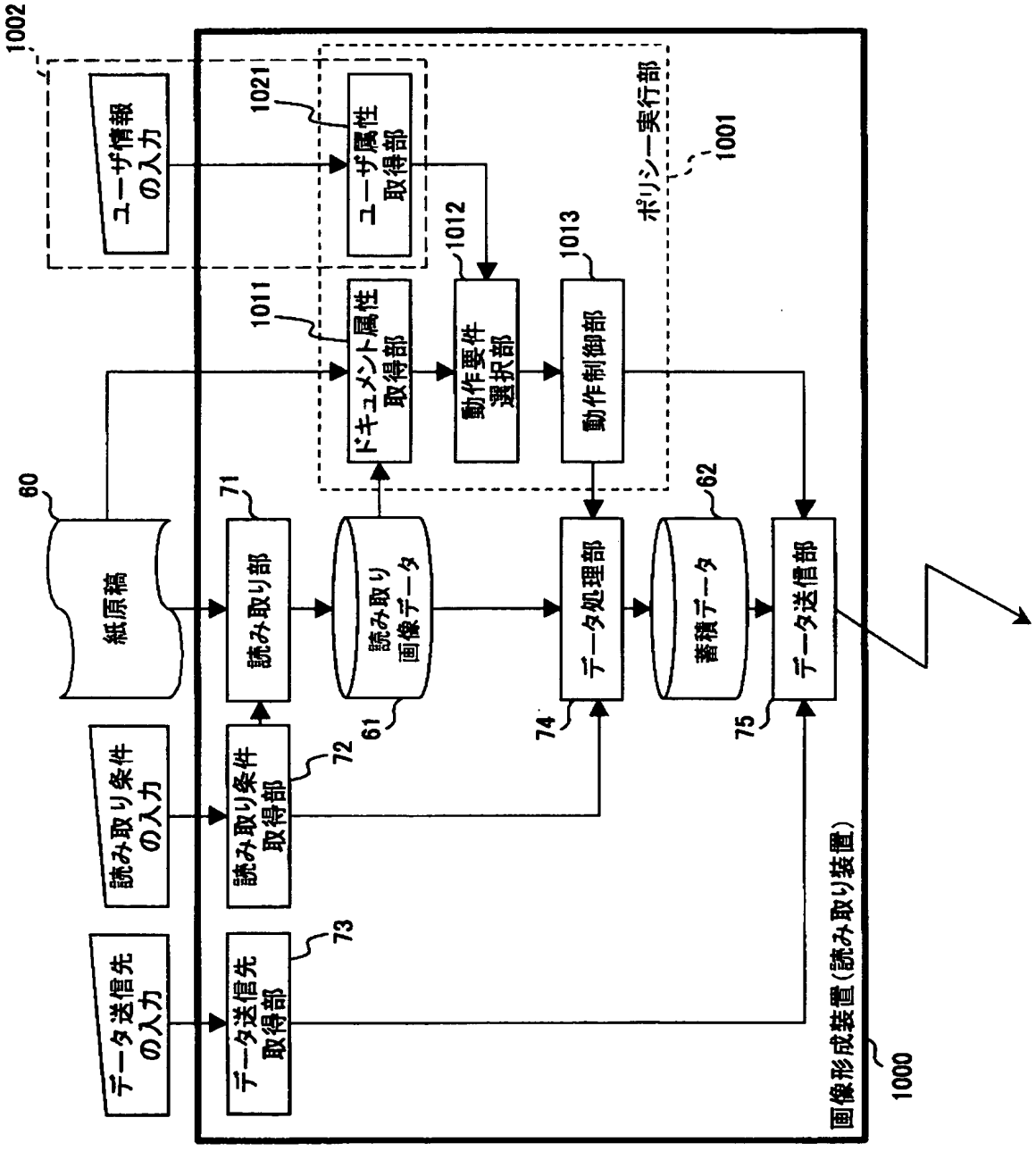
【図２７】

本発明の一実施例に係る画像形成装置の
ハードウェア構成を示すブロック図



【図２８】

セキュリティポリシーに従って動作する読み取り装置としての
画像形成装置の機能構成を示す図



【図２９】

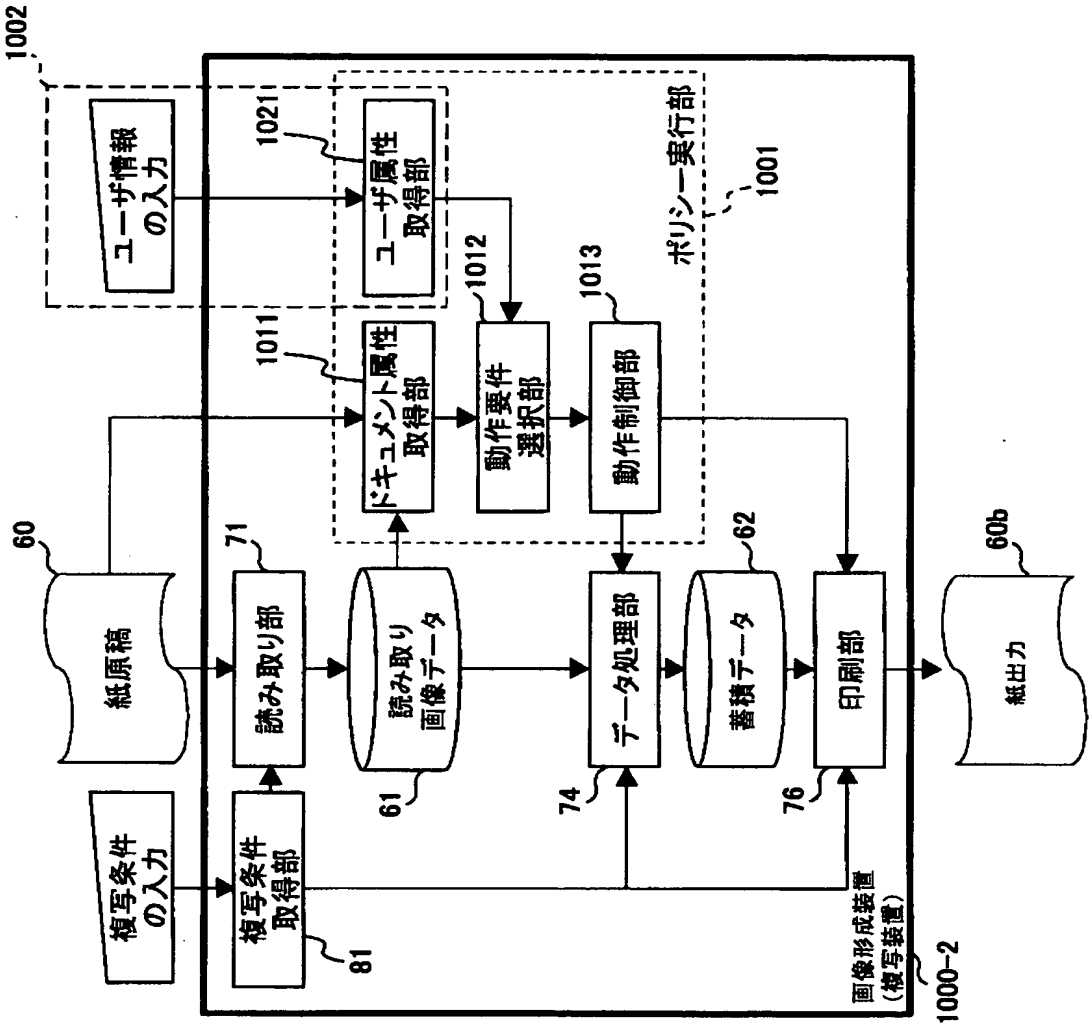
簡略化したDSPの例を示す図

2100

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
 <acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>basic</doc_security_level>
  <acl>
   <ace>
    <user_category>ANY</user_category>
    <user_security_level>ANY</user_security_level>
    <operation>
     <name>scan</name>
      <allowed/><!-- allowed without any requirement -->
     </operation>
     <operation>
      <name>net_delivery</name>
      <requirement>audit</requirement>
      <requirement>print_restriction</requirement>
      <requirement>trusted_channel</requirement>
     </operation>
    </ace>
   </acl>
  </acc_rule>
  <acc_rule>
   <doc_category>ANY</doc_category>
   <doc_security_level>high</doc_security_level>
   <acl>
    <ace>
     <user_category>DOC-CATEGORY</user_category>
     <user_security_level>ANY</user_security_level>
     <operation>
      <name>scan</name>
      <requirement>audit</requirement>
      <requirement>embed_trace_info</requirement>
     </operation>
    </ace>
   </acl>
  </acc_rule>
 </policy>
```

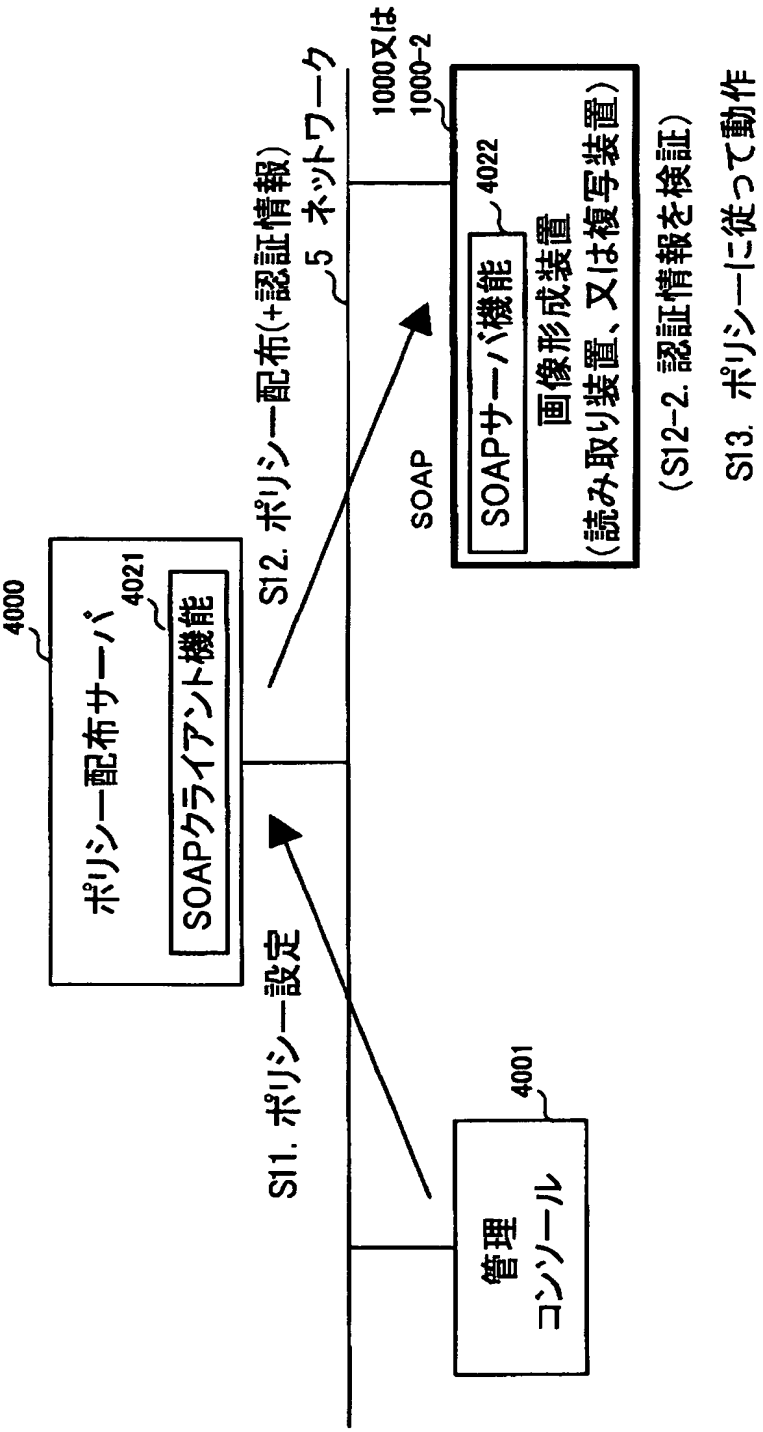
【図３０】

セキュリティポリシーに従って複写装置としての
画像形成装置の機能構成を示す図



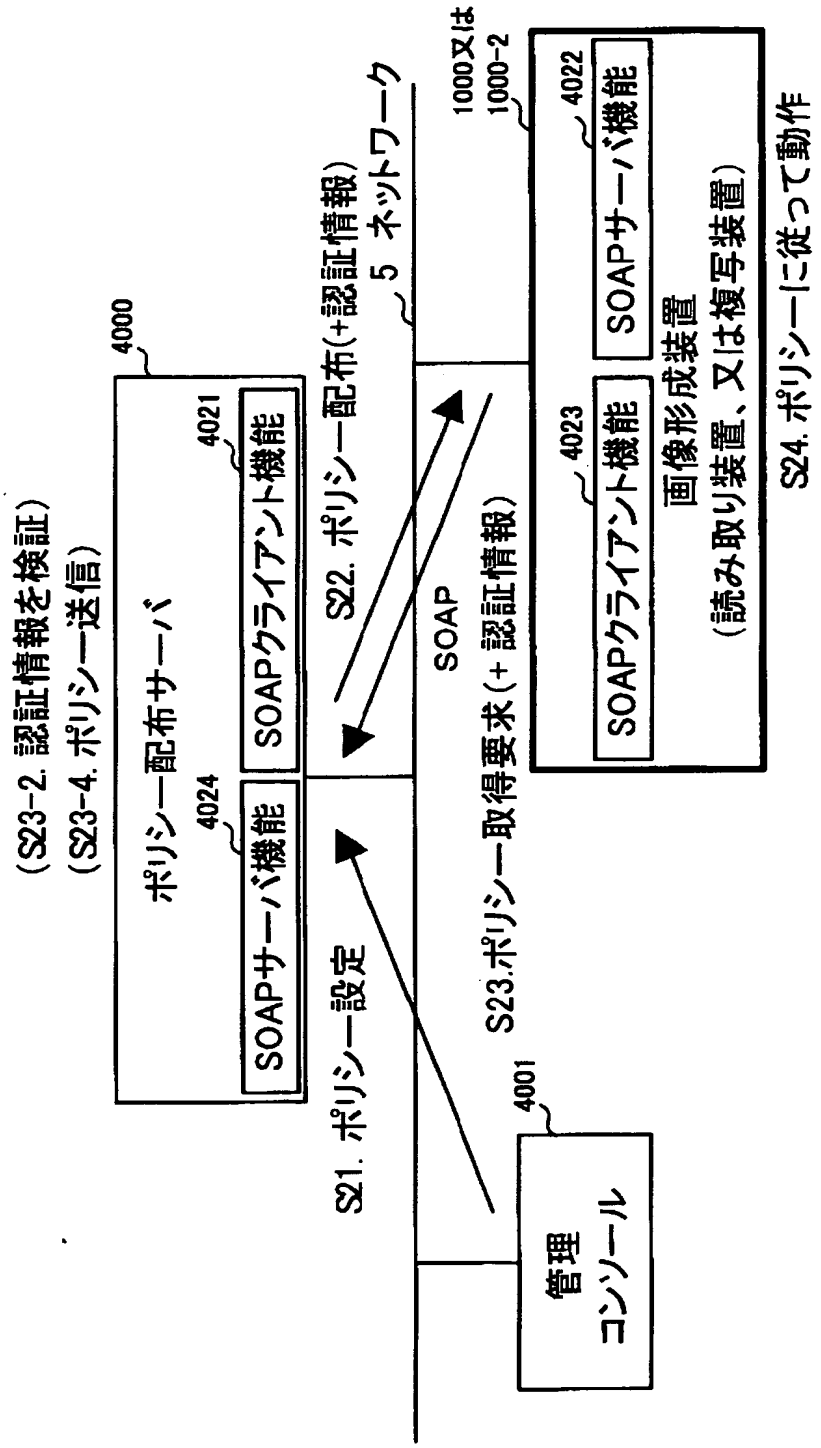
【図３１】

外部サーバからポリシーが配布される
第一のポリシー設定方法を示す図



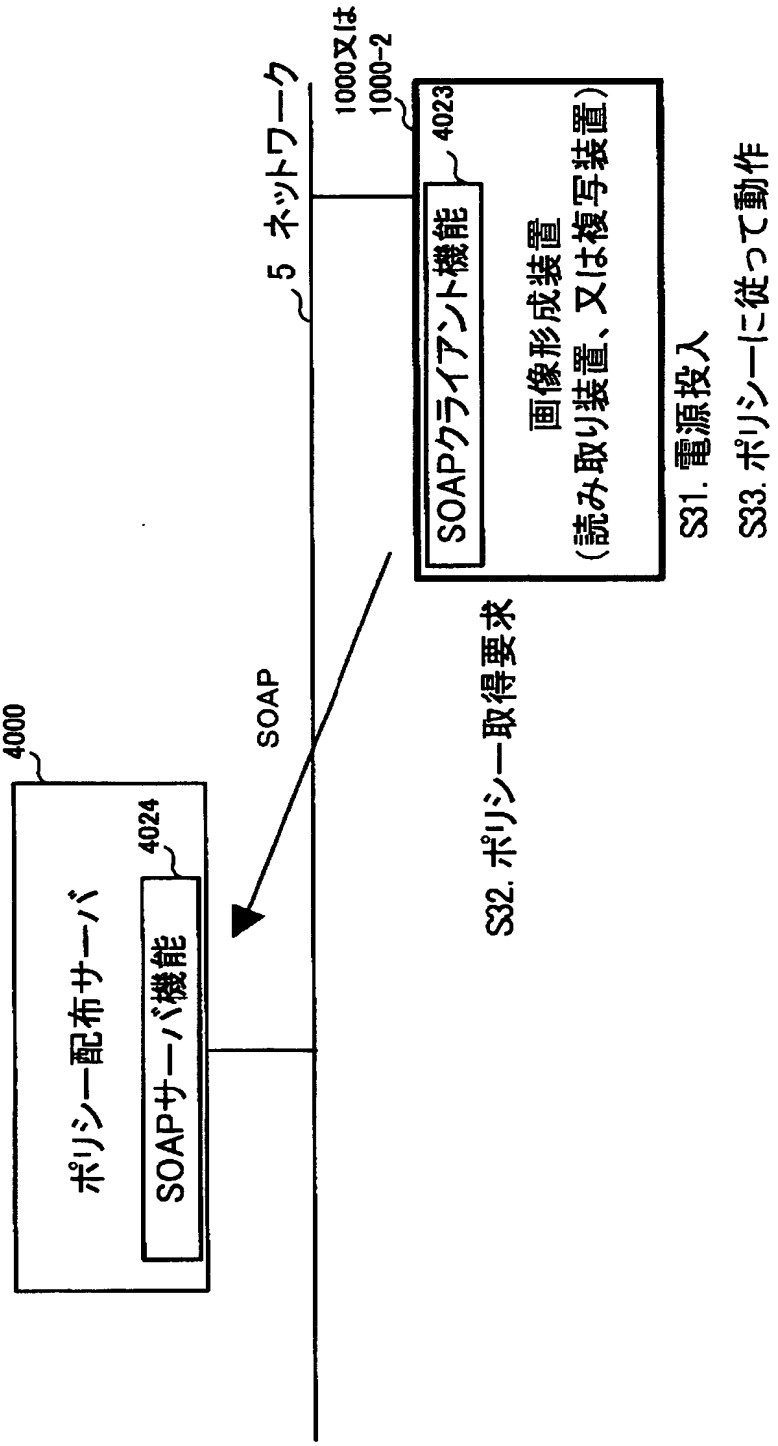
【図３２】

外部サーバからポリシーを取得する
第二のポリシー設定方法を示す図



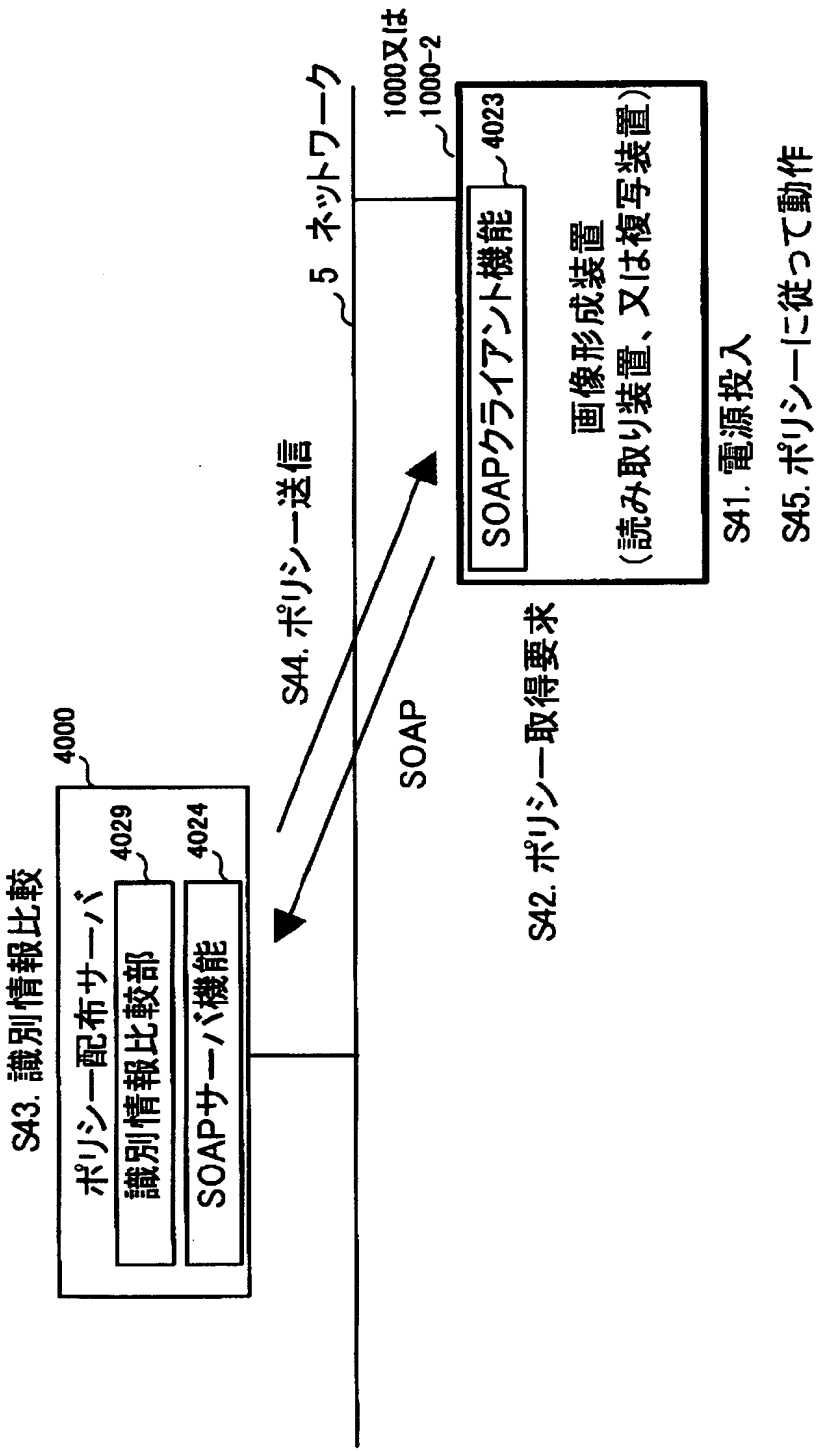
【図３３】

電源投入時にポリシーを取得する
第三のポリシー設定方法を示す



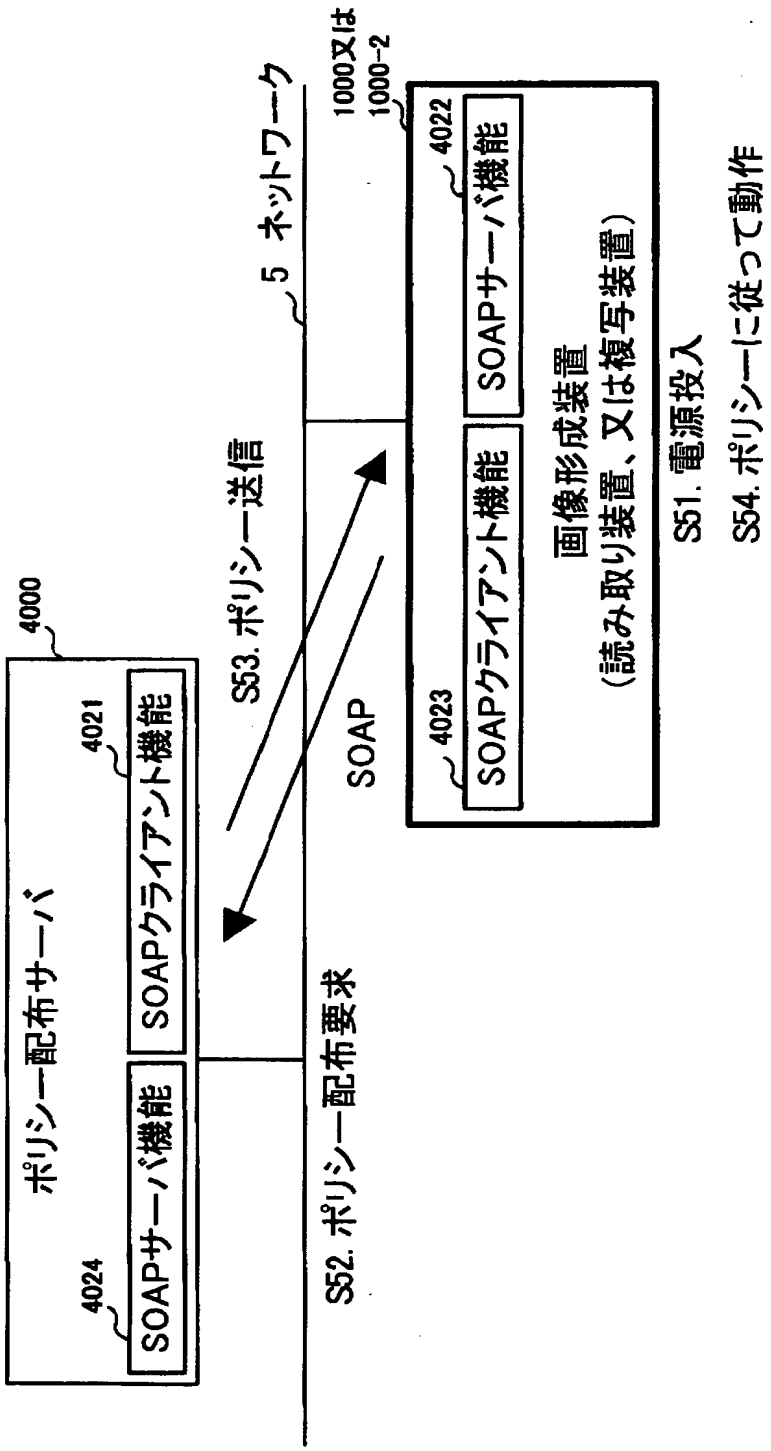
【図３４】

電源投入時にポリシー配布要求を行う
第四のポリシー設定方法を示す図



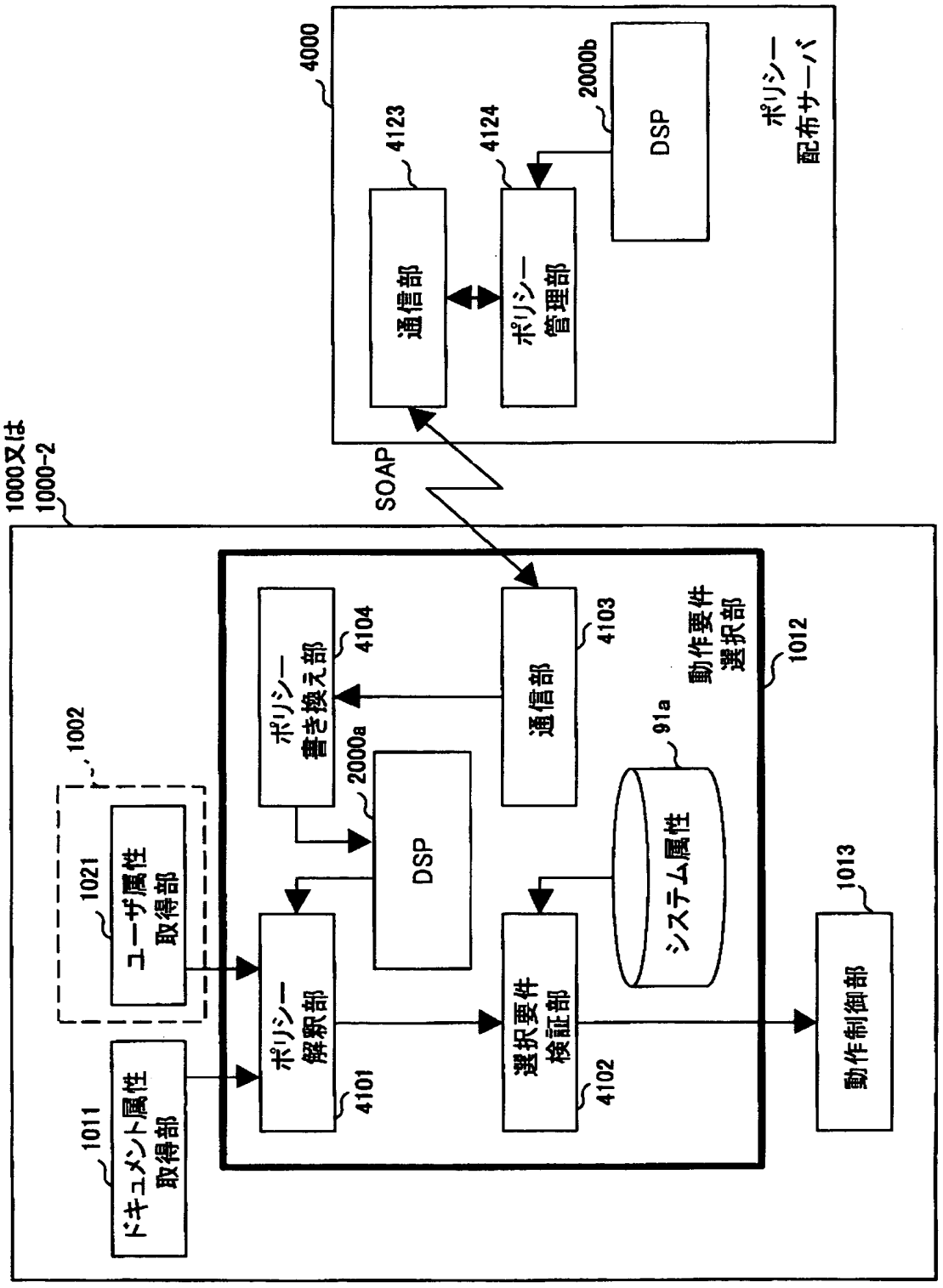
【図３５】

電源投入時にポリシー配布要求を行う
第五のポリシー設定方法を示す図



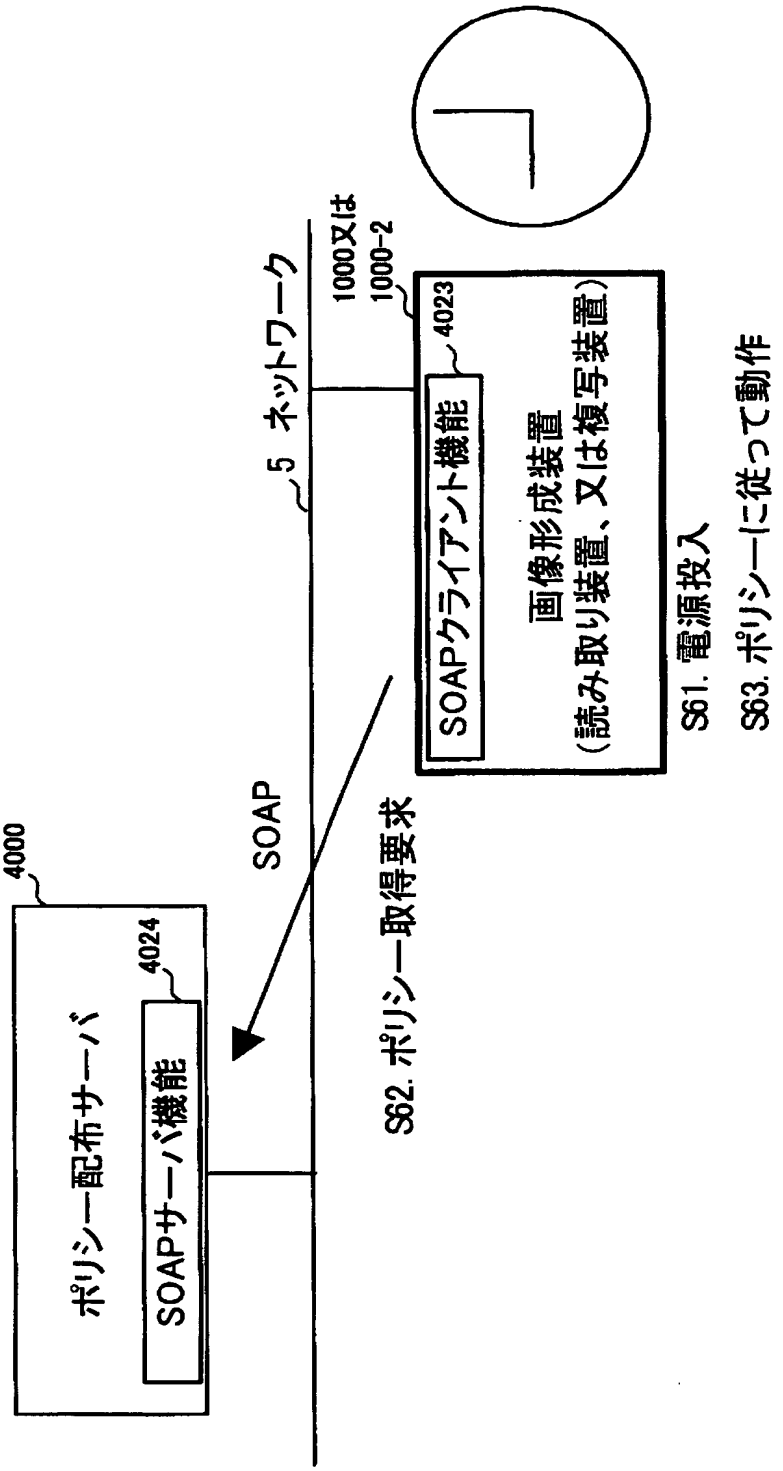
【図３６】

第一から第五のポリシー設定方法を実現するための機能構成の例を示す図



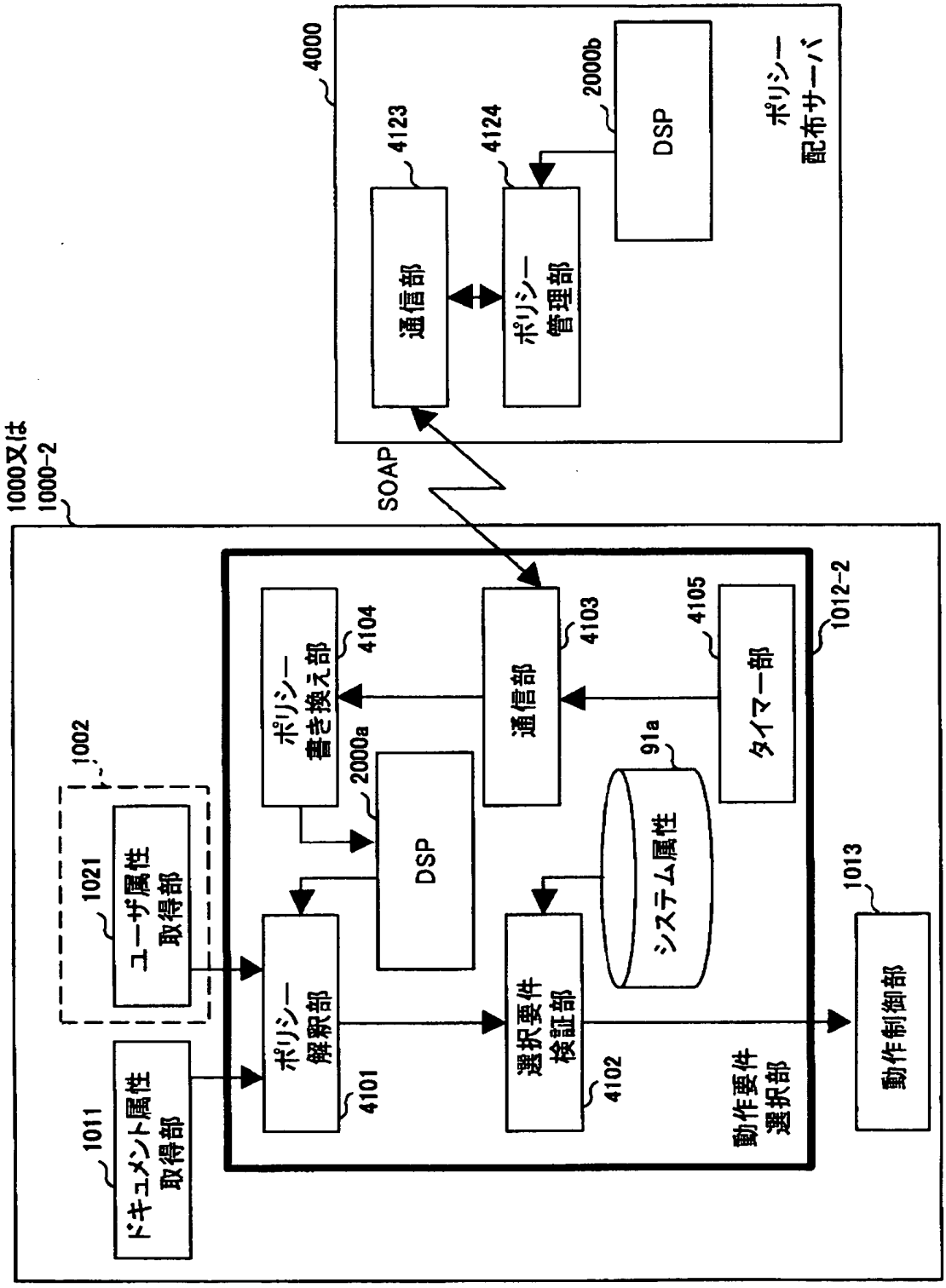
【図３７】

タイマーによってポリシーを取得する
第六のポリシー設定方法を示す図



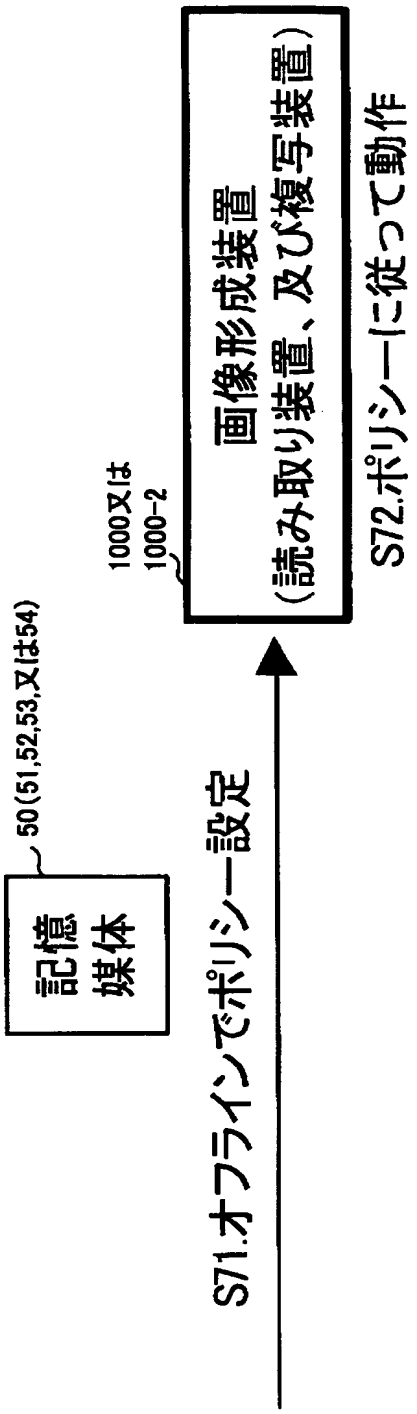
【図３８】

第六のポリシー設定方法を実現するための
機能構成の例を示す図



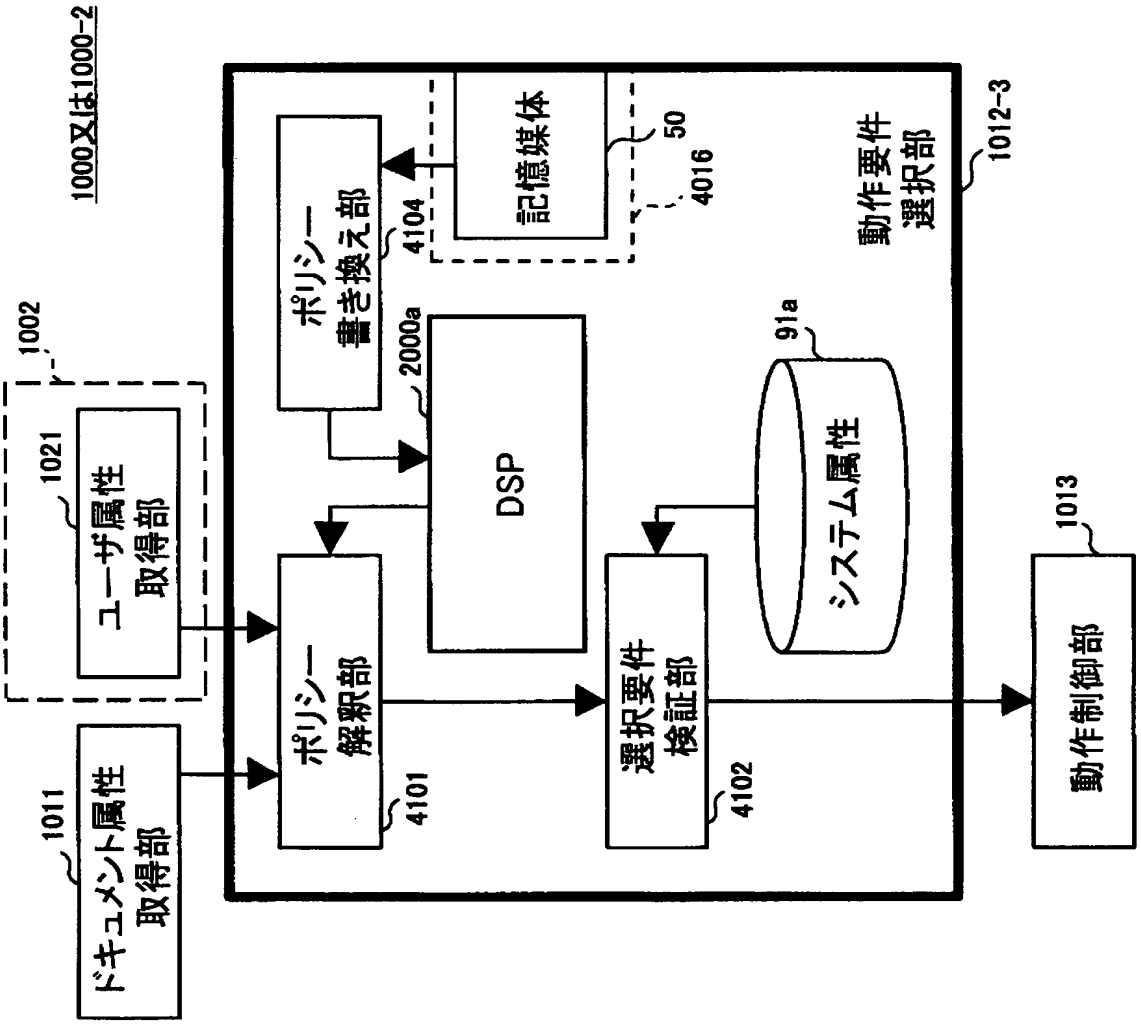
【図３９】

オフラインでポリシーを設定する
第七のポリシー設定方法を示す図



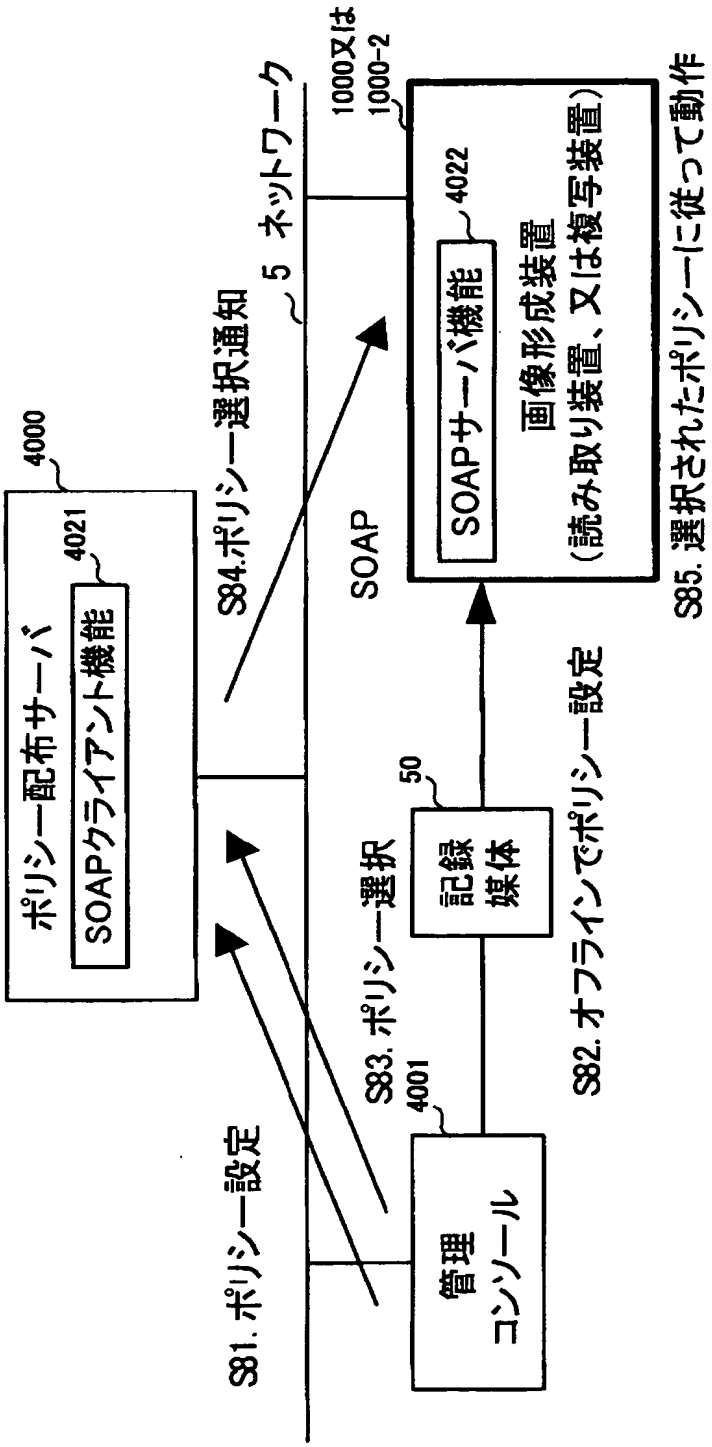
【図４０】

第六のポリシー設定方法を実現するための
機能構成の例を示す図



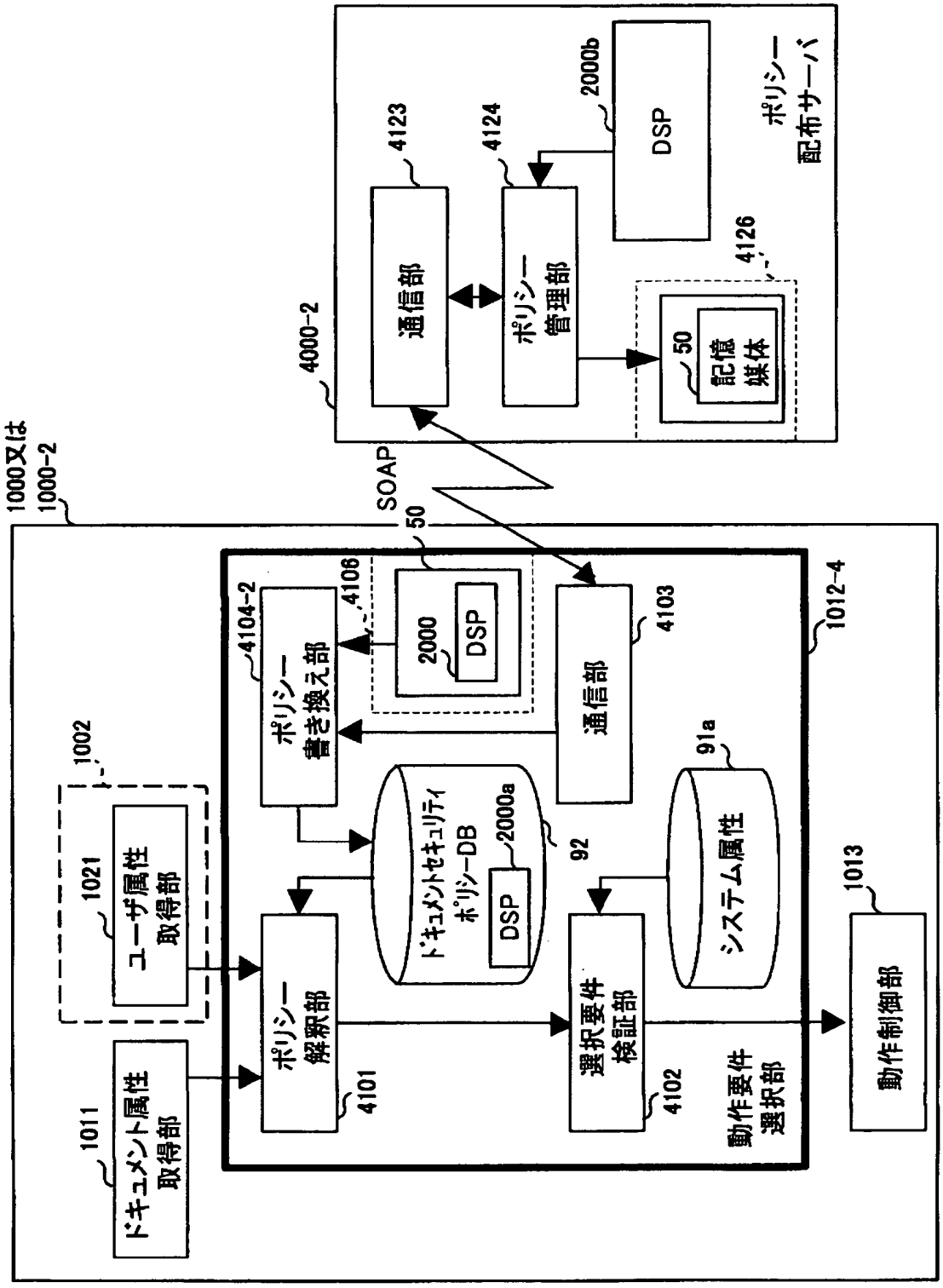
【図４１】

ポリシーをオフラインで設定し、オンラインで選択する
第八のポリシー設定方法を示す図



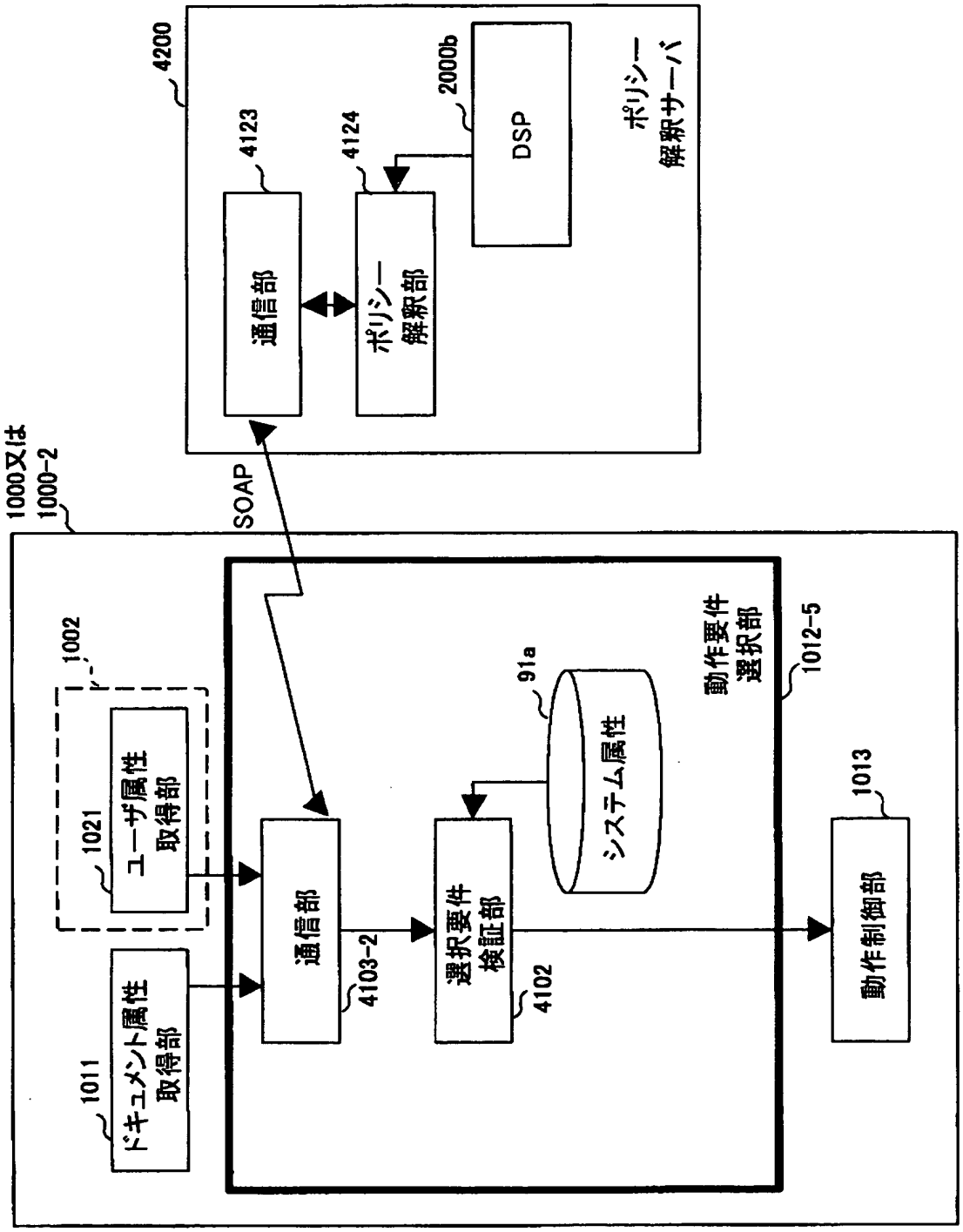
【図４２】

第八のポリシー設定方法を実現するための機能構成の例を示す図



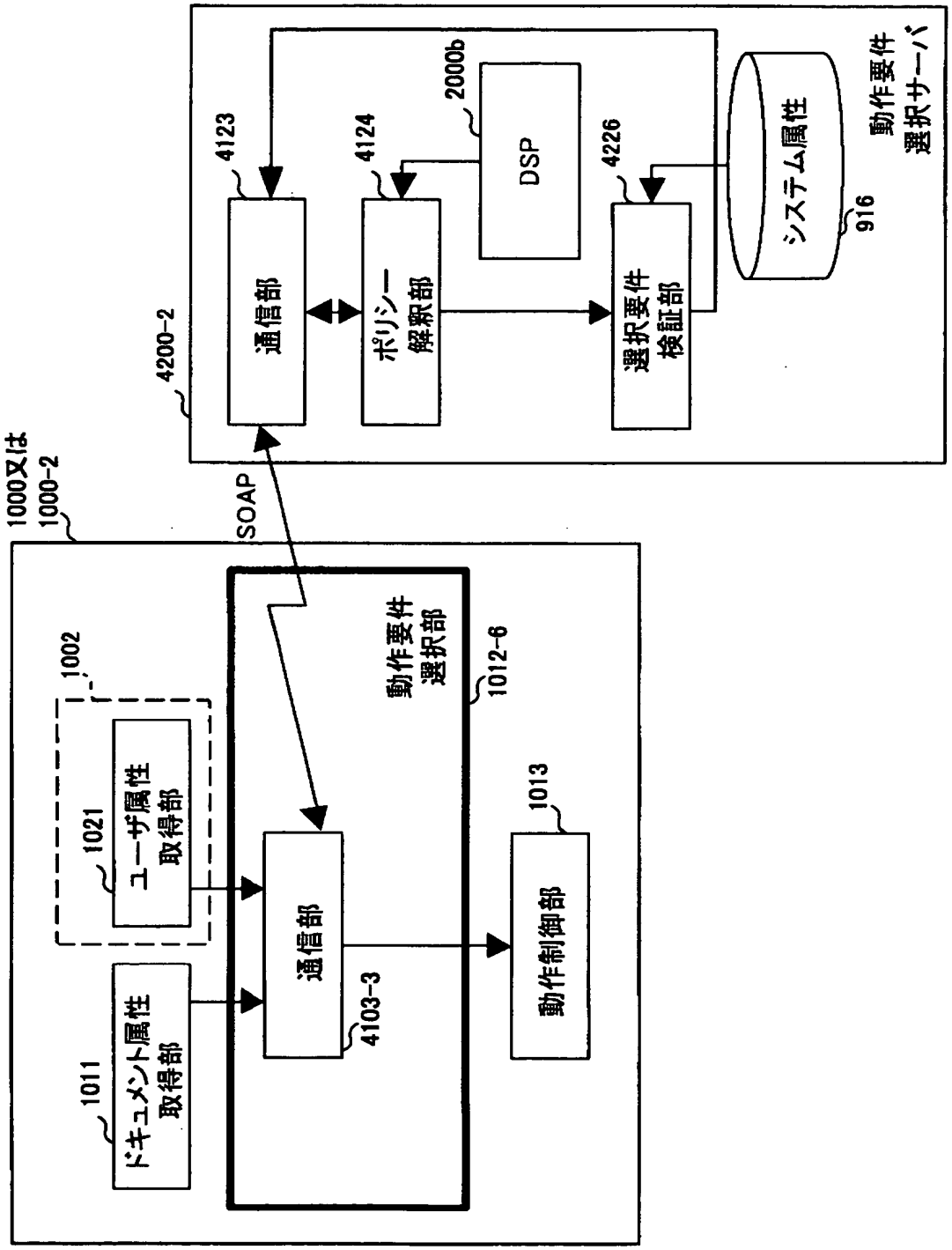
【図４３】

外部サーバがポリシーを解釈する機能構成の例を示す図



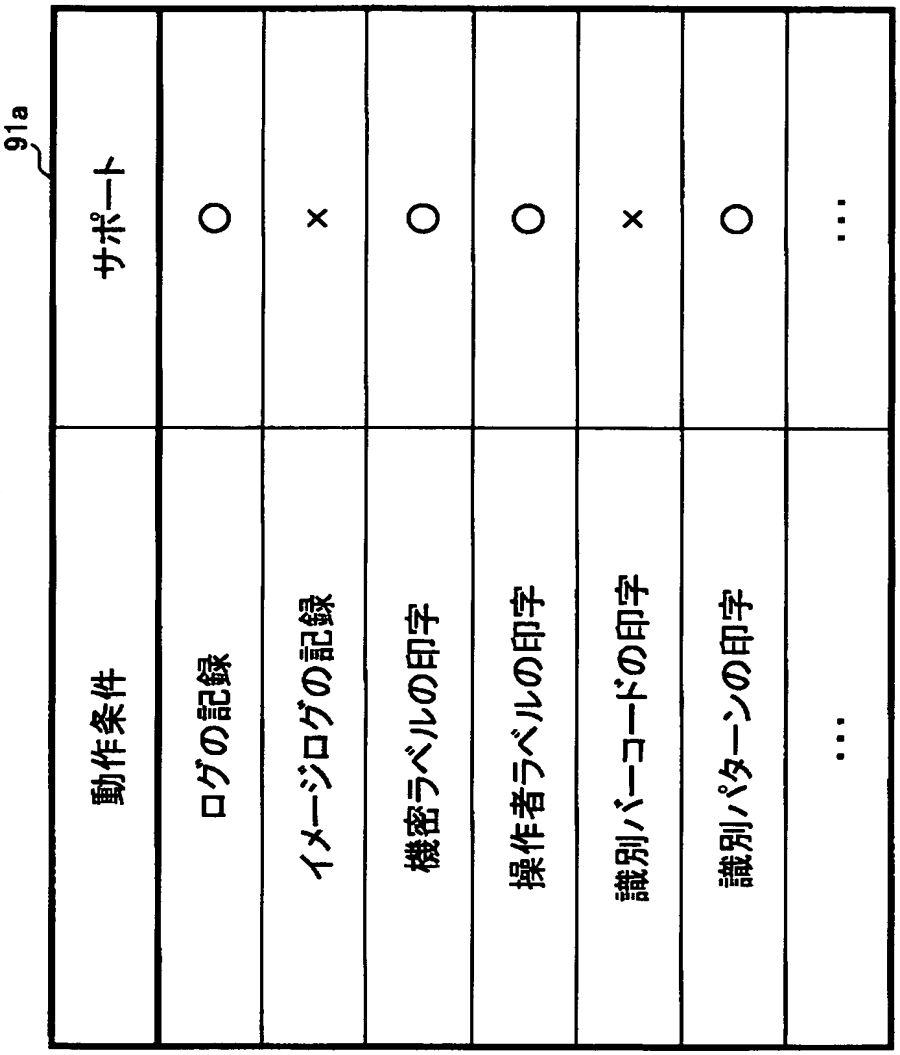
【図４４】

外部サーバがポリシーを解釈し、
選択要件を検証する機能構成の例を示す図



【図４５】

画像形成装置内に備えられたシステム属性の例を示す図



【図４６】

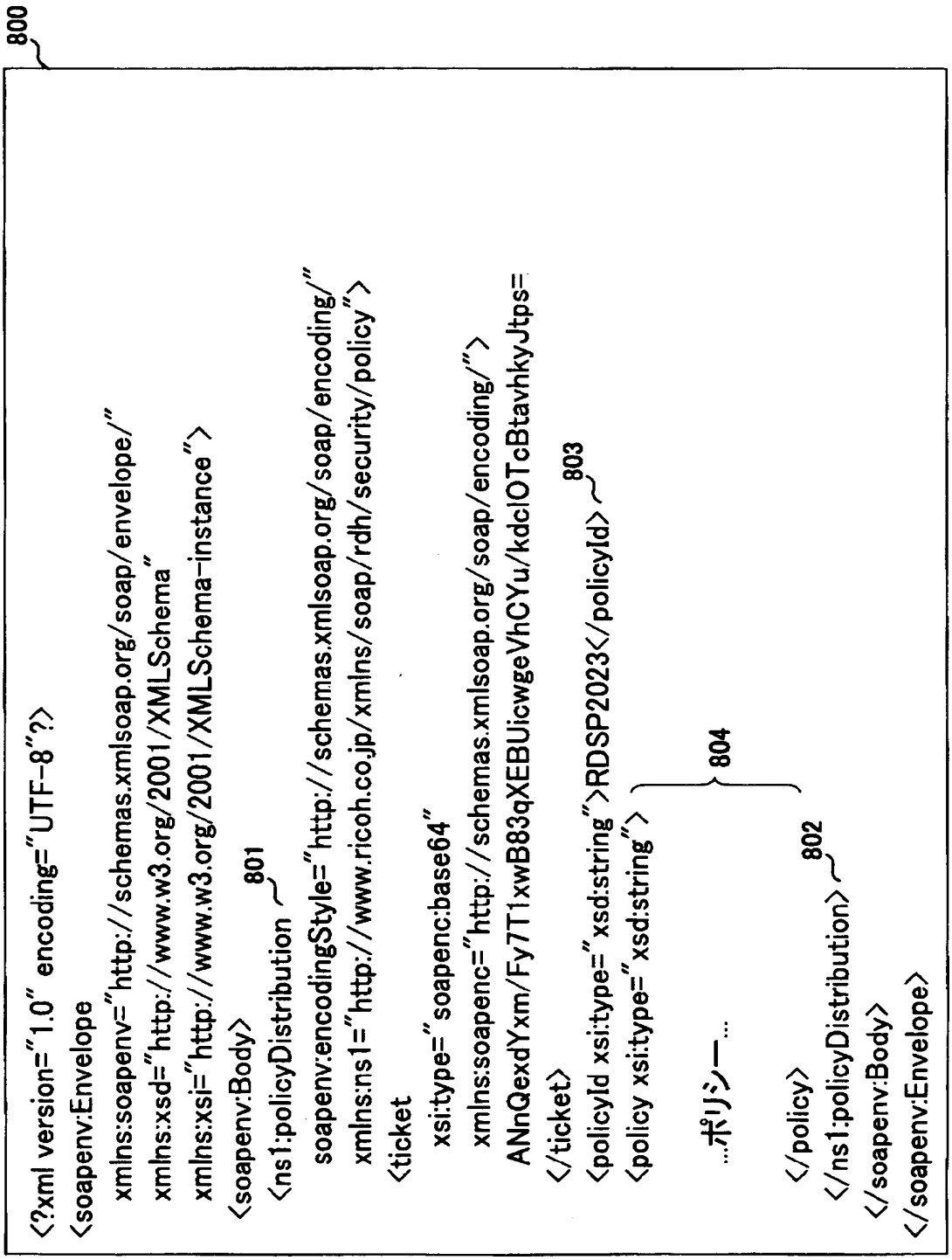
外部サーバに備えられたシステム属性の例を示す図

91b

動作条件	装置01	装置02	装置03	装置04	…
ログの記録	○	○	○	○	
イメージログの記録	×	×	○	○	
機密ラベルの印字	○	○	○	○	
操作者ラベルの印字	○	×	○	×	
識別バーコードの印字	×	×	○	×	
識別パターンの印字	○	×	○	×	
…	…	…	…	…	…

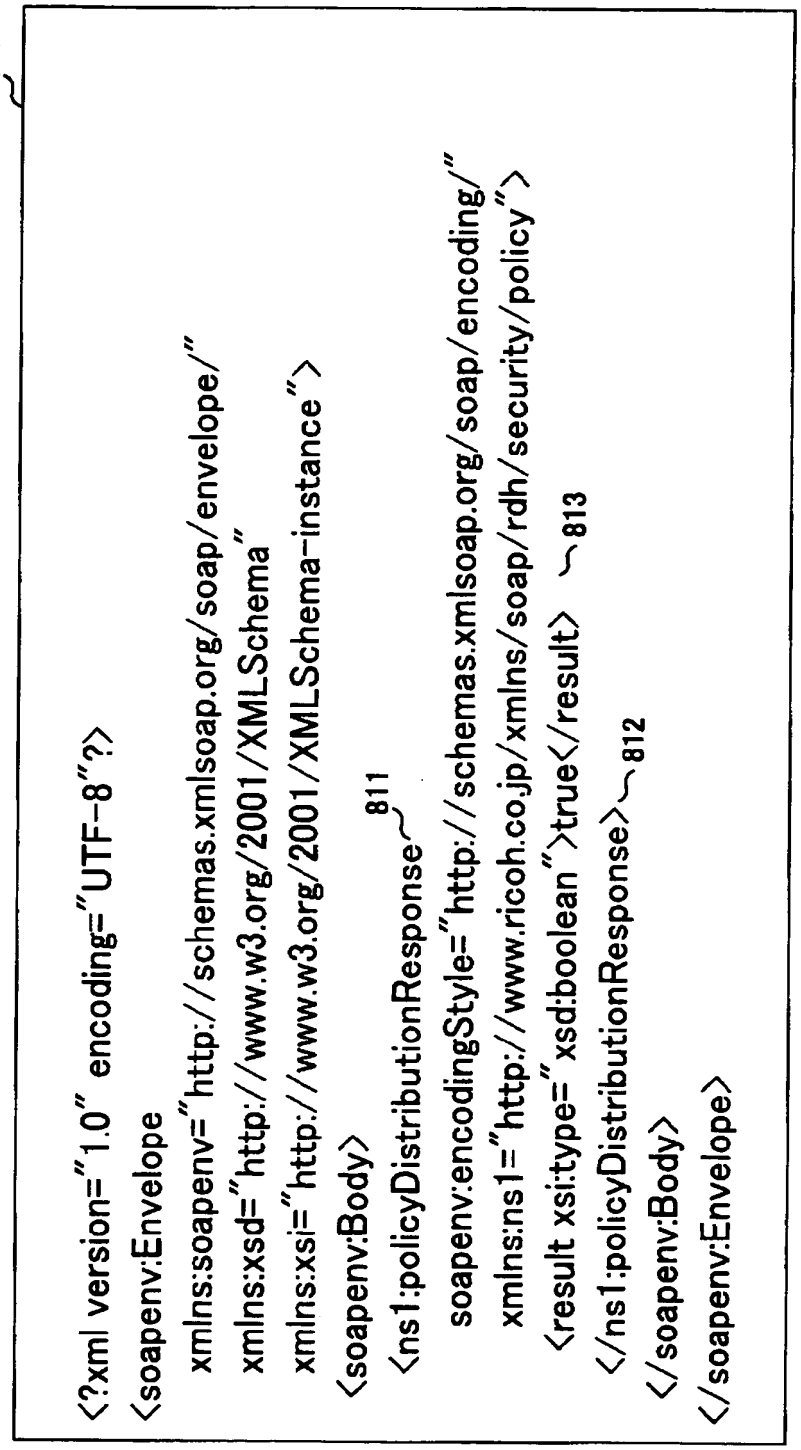
【図４７】

SOAPに従って送信されるポリシー配布を示す
XMLデータの例を示す図



【図４８】

SOAPに従って送信されるポリシー配布に対する受信結果を示す
XMLデータの例を示す図



【図４９】

SOAPに従って送信されるポリシー配布通知を示す
XMLデータの例を示す図

820

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
    xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
  <ns1:policyDistributionReport                    821
      soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
      xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
    <ticket
        xsi:type="soapenc:base64"
        xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
      ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdclOTcBtavhkyJtps=
    </ticket>
    <policyId xsi:type="xsd:string">RDSP2023</policyId>   823
  </ns1:policyDistributionReport>                  822
</soapenv:Body>
</soapenv:Envelope>
```

【図５０】

SOAPに従って送信されるポリシー取得要求を示す
XMLデータの例を示す図

830

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:policyRequest                                    831
    soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
    xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
   <ticket
     xsi:type="soapenc:base64"
     xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
     ANnQexdYxm/shuqjlKsy73kahqw520iUsJqlhHKJ/kdclOTcBtavhkyJtps=
   </ticket>
   <policyId xsi:type="xsd:string">RDSP2023</policyId>  833
  </ns1:policyRequest>                                  832
 </soapenv:Body>
</soapenv:Envelope>
```

【図５１】

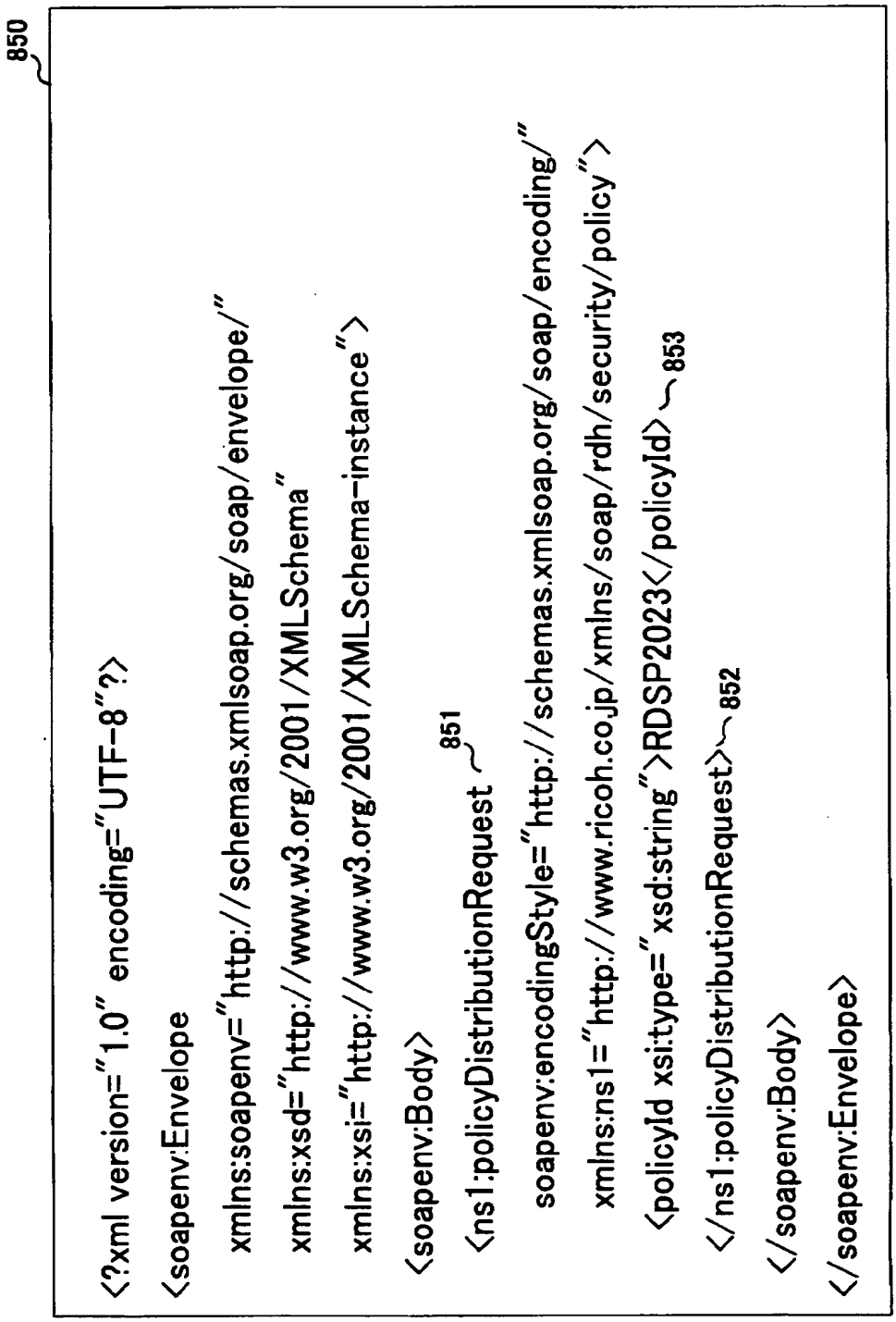
SOAPに従って送信されるポリシー取得要求に対する
受信結果を示すXMLデータの例を示す図

840

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>                                          841
 <ns1:policyDistribution
    soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
    xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
  <ticket
     xsi:type="soapenc:base64"
     xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  </ticket>
  <policyId xsi:type="xsd:string">RDSP2023</policyId>          843
  <policy xsi:type="xsd:string">                          844
     ...ポリシー...
  </policy>
 </ns1:policyDistribution>                                842
</soapenv:Body>
</soapenv:Envelope>
```

【図５２】

SOAPに従って送信されるポリシー配布要求を示すXMLデータの例を示す図



【図５３】

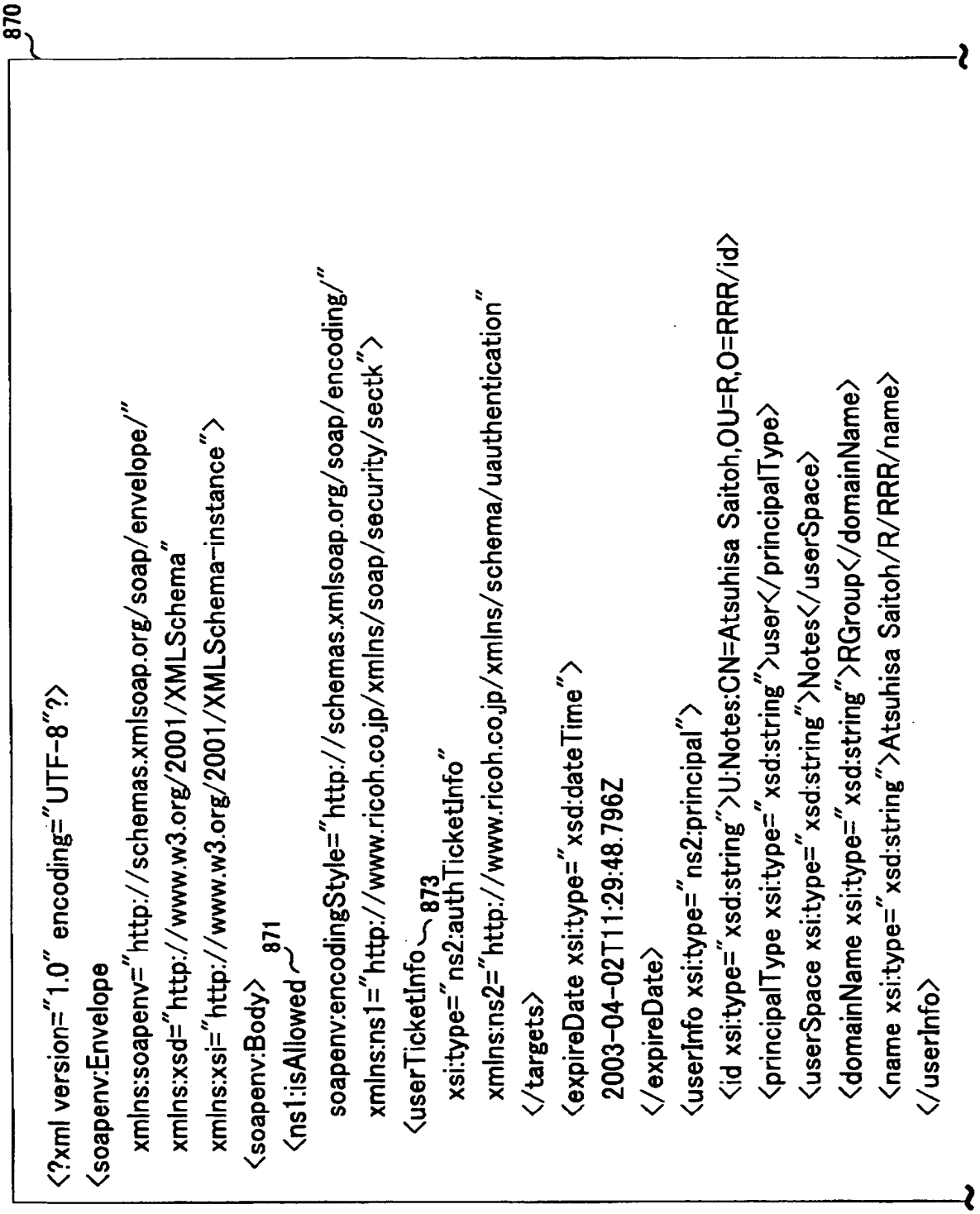
SOAPに従って送信されるポリシー選択通知を示す
XMLデータの例を示す図

860

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>
<ns1:policyChangeRequest                                    861
   soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
   xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/policy">
   <ticket
      xsi:type="soapenc:base64"
      xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
      ANnQexdYxm/Fy7T1xwB83qXEBUicwgeVhCYu/kdclOTcBtavhkyJtps=
   </ticket>
   <policyId xsi:type="xsd:string">RDSP2023</policyId>      863
</ns1:policyChangeRequest>                                  862
</soapenv:Body>
</soapenv:Envelope>
```

【図５４】

SOAPに従って送信される動作要件取得要求を示す
XMLデータの例を示す図



【図５５】

SOAPに従って送信される動作要件取得要求を示す
XMLデータの例を示す図

```
<groupInfo
  xsi:type="soapenc:Array"
  soapenc:arrayType="ns2:principal[1]"
  xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
  <item>
    <id xsi:type="xsd:string">G:Notes:CN=PBDSS_USERS</id>
    <principalType xsi:type="xsd:string">group</principalType>
    <userSpace xsi:type="xsd:string">Notes</userSpace>
    <domainName xsi:type="xsd:string">RGroup</domainName>
    <name xsi:type="xsd:string">PBDSS_USERS</name>
  </item>
</groupInfo>                                          874
</userTicketInfo>
<docInfo xsi:type="ns1:DocInfo"                       882
  <catgory xsi:type="xsd:string">Technical_doc/category>
  <level xsi:type="xsd:string">High</level>           883
  <zone xsi:type="xsd:string">99.99.99.99</zone>      884
</docInfo>
<accessInfo
  xsi:type="ns3:AccessInfo"
  xmlns:ns3="http://www.rrr.co.jp/xmlns/schema/security/policy"
  <operation xsi:type="xsd:string">COPY</operation>   886
</accessinfo>
</ns1:isAllowed>                                      872
</soapenv:Body>
</soapenv:Envelope>
```

881
885

【図５６】

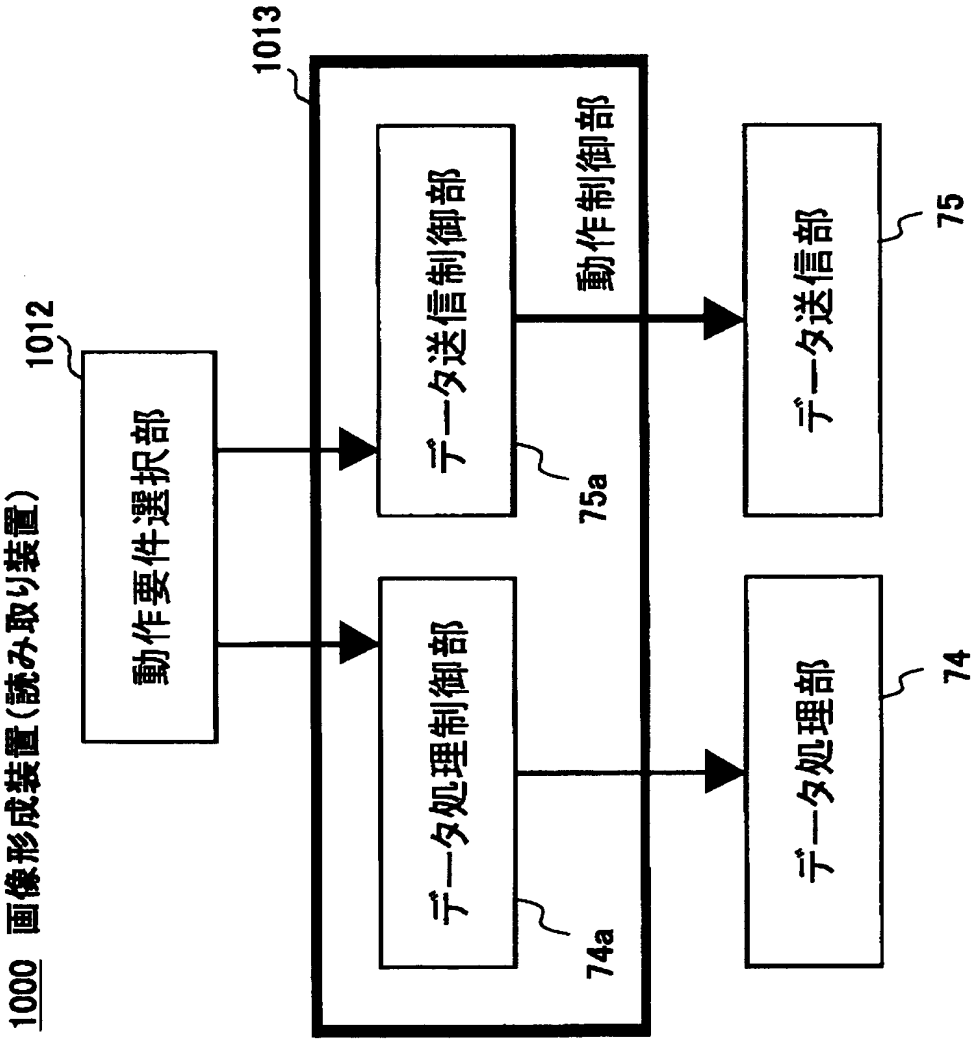
SOAPに従って送信されるポリシー解釈結果を示す
XMLデータの例を示す図

890

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
   xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<soapenv:Body>                                          891
 <ns1:isAllowedResponse
    soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
    xmlns:ns1="http://www.ricoh.co.jp/xmlns/soap/rdh/security/sectk">
  <isAllowedReturn
     xsi:type="ns2:DecisionInfoEx"
     xmlns:ns2="http://www.ricoh.co.jp/xmlns/schema/rdh/security/sectk">
    <allowed xsi:type="xsd:boolean">true</allowed>          895
    <requirements
       xsi:type="soapenc:Array"
       soapenc:arrayType="ns3:Requirement[1]"
       xmlns:ns3="http://www.ricoh.co.jp/xmlns/schema/rdh/security/policy"
       xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
     <item>                                                 897
      <requirement xsi:type="xsd:string">audit</requirement>
     </item>                                                896
    </requirements>
   </isAllowedReturn>                                       892
  </ns1:isAllowedResponse>
 </soapenv:Body>
</soapenv:Envelope>
```

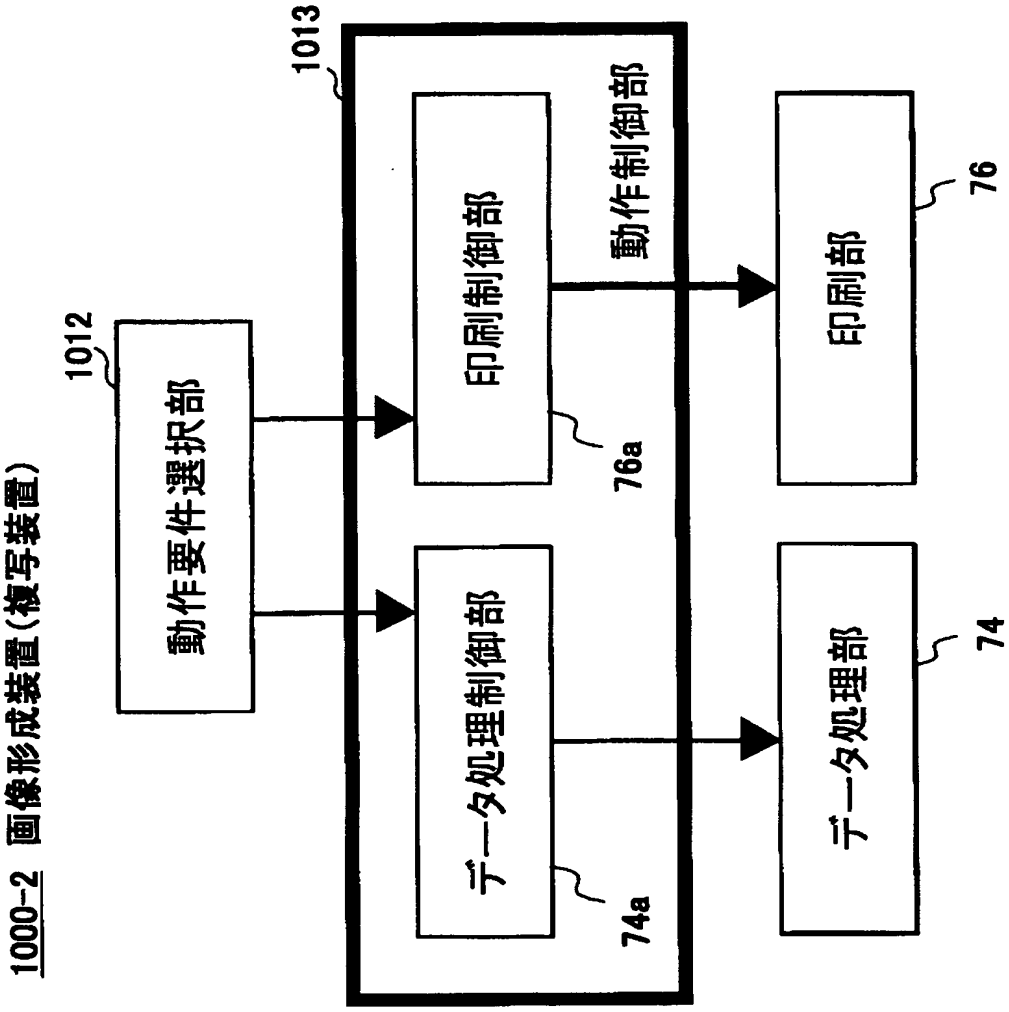
【図５７】

読み取り装置としての画像形成装置における
動作制御部の機能構成の例を示す図



【図５８】

複写装置としての画像形成装置における
動作制御部の機能構成の例を示す図



【書類名】要約書
【要約】
【課題】　本発明の課題は、情報システムのセキュリティを確保するシステムに関し、特に、ドキュメントのドキュメント属性を取得することによって、セキュリティポリシーに基づいた処理制御を行う画像形成装置を提供することを目的とする。
【解決手段】　本発明の課題は、ドキュメントに関する取り扱いのルールを記述したセキュリティポリシーを保持するポリシー保持手段と、外部からのセキュリティポリシーで上記ポリシー保持手段にて保持される上記セキュリティポリシーを書き換えるポリシー書き換え手段と、上記ポリシー管理手段によって管理される上記セキュリティポリシーに従って、上記ドキュメントに対する動作を制御する動作制御手段とを有する画像形成装置によって達成される。
【選択図】　図３６

特願２００３－３１４４６５

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー